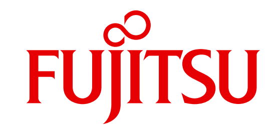
Benutzerhandbuch - Deutsch



HNC Software V2.0

High-Speed Network Connect

HNC-V 91854
HNC-IV 91853

Ausgabe Februar 2011

Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2008

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2008 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright und Handelsmarken

Das Linux-basierte Basissystem des HNC enthält Open-Source-Software. Die Lizenzen dazu finden Sie auf der jeweiligen Installations-DVD im Verzeichnis LICENSES.

Inhalt

1 Einleitung . . . 7

1.1 Zielsetzung und Zielgruppen des Handbuchs . . . 7

1.2 Konzept des Handbuchs . . . 7

1.3 Änderungen gegenüber dem Vorgänger-Handbuch . . . 8

1.4 Open-Source-Software . . . 8

1.5 Darstellungsmittel . . . 9

2 Architektur . . . 11

2.1 Prinzipielle Arbeitsweise . . . 13
2.1.1 LAN-Anbindung des HNC . . . 15
2.1.2 BS2000-Anschlüsse und emulierte BS2000-Geräte . . . 15

2.2 Hardware . . . 16

2.3 Software . . . 17

3 HNC bedienen . . . 19

3.1 HNC-Manager . . . 19
3.1.1 HNC-Manager aufrufen . . . 20
3.1.2 Anmelden . . . 20
3.1.3 Abmelden . . . 21
3.1.4 Session-Verwaltung . . . 21
3.1.5 Oberfläche des HNC-Managers . . . 22
3.1.5.1 Fenster-Typen . . . 22
3.1.5.2 Hauptfenster . . . 23
3.1.5.3 Dialoge . . . 25
3.1.6 Objekt oder Funktion aufrufen . . . 26
3.1.7 Navigieren . . . 27

3.1.8 Tabelle filtern . . . 27
3.1.9 Tabelle sortieren . . . 27
3.1.10 Online-Hilfe aufrufen . . . 28
3.1.11 Fehlerbehandlung . . . 30

3.2 Zugang zum CLI . . . 31
3.2.1 Terminal-Fenster öffnen . . . 31
3.2.2 Terminal-Fenster schließen . . . 31
3.2.3 Kommandos . . . 32
3.2.3.1 auditLog . . . 32
3.2.3.2 cli_info . . . 32
3.2.3.3 init . . . 32

4 BS2000-Anschlüsse . . . 33

5 HNC verwalten . . . 39

5.1 Informationen über den HNC einholen . . . 39

5.2 HNC konfigurieren . . . 41
5.2.1 Rechnernamen, Default-Gateway, LAN-Schnittstellen und DNS-Konfiguration verwalten . . . 41
5.2.2 Systemzeit konfigurieren . . . 42
5.2.3 SNMP konfigurieren . . . 43
5.2.4 Links auf externe Geräte verwalten . . . 45

5.3 Kennungen verwalten . . . 46
5.3.1 Lokale Kennungen verwalten . . . 46
5.3.2 Passwörter . . . 47
5.3.3 Zugang zu einem LDAP-Server einrichten . . . 48
5.3.4 LDAP-Kennungen verwalten . . . 49

5.4 CSR-Sicherungen verwalten . . . 50

5.5 HNC ein- und ausschalten . . . 52

6 Diagnose und Wartung . . . 53

6.1 Wartungskonzept . . . 53
6.1.1 Remote-Service . . . 53
6.1.2 Aufgaben des Service . . . 54
6.1.3 Aufgaben des Kunden . . . 55

6.2 Updates . . . 56
6.2.1 Aufgaben und Zuständigkeiten . . . 57
6.2.2 Updates beschaffen . . . 58
6.2.3 Updates verwalten . . . 58
6.2.4 Aktionen für Updates . . . 59

6.3 Den Service unterstützen . . . 59

6.4 Diagnosedaten . . . 60

6.5 Systemprotokoll (Auditlog) . . . 61

Literatur . . . 63

Stichwörter . . . 65

1 Einleitung

Das vorliegende Benutzerhandbuch beschreibt Architektur und Konzept des High-speed Network Connect (kurz: HNC). Der HNC verbindet S-Server mit dem LAN. Zu seiner Bedienung und Verwaltung bietet der HNC eine Web-Oberfläche, den HNC-Manager.

1.1 Zielsetzung und Zielgruppen des Handbuchs

Das Handbuch wendet sich an die Systembetreuung und an den Netzverwalter.

Voraussetzung sind Kenntnisse der BS2000-Systembedienung, BS2000-Systembetreuung und BS2000-Administration.

1.2 Konzept des Handbuchs

Die Dokumentation zum HNC mit Software-Stand 2.0 (HNC-V 91854 und HNC-IV 91853) besteht aus diesem Handbuch, dem Sicherheitshandbuch und aus der Online-Hilfe.

- Das Handbuch gibt einen Überblick über die Architektur und Konzepte des HNC und stellt seine Funktionen vor.
- Das Sicherheitshandbuch [6], das auch für den SQ-Server und den SKP gilt, enthält die sicherheitsrelevanten Aspekte für den HNC.
- Die Online-Hilfe beschreibt alle Funktionen des HNC-Managers. Die Online-Hilfe öffnen Sie im HNC-Manager, siehe auch Online-Hilfe aufrufen.

Das Handbuch ist wie folgt aufgebaut:

Das Kapitel „Architektur“ stellt schematisch die Architektur und Hardware des HNC sowie die Verbindungen zum S-Server dar.

Das Kapitel „HNC bedienen“ erklärt den Aufbau der Web-Oberfläche und den Zugang zum HNC über die CLI (Command Line Interface).

Das Kapitel „BS2000-Anschlüsse“ beschreibt die Hauptfunktion des HNCs, BS2000-Anschlüsse zu überwachen und gegebenenfalls neu zu starten.

Das Kapitel „HNC verwalten“ beschreibt, wie Sie den HNC über die Funktionen des HNC-Management im HNC-Manager verwalten.

Das Kapitel „Diagnose und Wartung“ beschreibt, wie Sie den HNC warten und im Fehlerfall vorgehen.

Im Anschluss daran finden Sie ein Literatur- und ein Stichwortverzeichnis.

Weiterführende Literatur

Für das prinzipielle Verständnis von BS2000/OSD werden die Handbücher „Systeminstallation“ [1] und „Einführung in die Systembetreuung“ [2] empfohlen.

Für das prinzipielle Verständnis von VM2000 wird das Handbuch „VM2000“ [3] empfohlen.

Für weitere Information über das Datenkommunikationssystem BCAM wird das Handbuch „openNet Server BCAM“ [4] empfohlen.

Die im Handbuch genannten BS2000/OSD-Kommandos werden im Handbuch „Kommandos“ [5], die VM2000-Kommandos im Handbuch „VM2000“ [3] beschrieben.

Die Bedienung der S-Server ist in den jeweiligen Betriebsanleitungen „Business Server Sxxx“ beschrieben.

Die Bedienung des PRIMERGY-Servers der Serie TX300, der als Hardware-Basis für den HNC dient, ist in der entsprechenden Betriebsanleitung beschrieben.

Literaturhinweise werden im Text in Kurztiteln angegeben. Der vollständige Titel jeder Druckschrift, auf die durch eine Nummer in eckigen Klammern verwiesen wird, ist im Literaturverzeichnis hinter der entsprechenden Nummer aufgeführt.

1.3 Änderungen gegenüber dem Vorgänger-Handbuch

Das vorliegende Handbuch wurde komplett überarbeitet und den neuen Funktionen des HNC angepasst.

1.4 Open-Source-Software

Das Linux-basierte Basissystem des HNC enthält Open-Source-Software. Die Lizenzen dazu finden Sie auf der jeweiligen Installations-DVD im Verzeichnis LICENSES.

1.5 Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

i	Kennzeichnet wichtige Informationen und Tipps.
!	Kennzeichnet eine Warnung vor Datenverlust.
►	Kennzeichnet einen Arbeitsschritt, den Sie ausführen müssen.
Kursive Schrift	Kennzeichnet Zitate aus der Web-Oberfläche.
`dicktengleich`	Kennzeichnet Systemein- und ausgaben.
`dicktengleich halbfett`	Kennzeichnet über die Tastatur einzugebende Anweisungen.
VERSALIEN	Kennzeichnet BS2000-Kommandos.
<abc>	Kennzeichnet Variablen, die durch Werte ersetzt werden.
[Tastensymbole]	Tasten werden entsprechend ihrer Abbildung auf der Tastatur dargestellt. Wenn explizit Großbuchstaben eingegeben werden sollen, so wird die Shift-Taste angegeben, z. B. [SHIFT] - [A] für A. Müssen zwei Tasten gleichzeitig gedrückt werden, so wird dies durch einen Bindestrich zwischen den Tastensymbolen gekennzeichnet.

Tabelle 1: Darstellungsmittel

In diesem Handbuch werden folgende Kurzbezeichnungen verwendet:

- S-Server für die Business Server der S-Serie (/390-Architektur)
- BS2000 für das Betriebssystem BS2000/OSD in Wortverbindungen, z.B. BS2000-System.

2 Architektur

Der HNC (High-speed Network Connect) verbindet das BS2000/OSD-System (oder die BS2000/OSD-Systeme) eines S-Servers mit dem LAN (Verbindungstyp ZASLAN). Der S-Server kann dafür über Fibre Channel (FC) oder über ESCON (nur auf der Hardware des HNC-IV 91853) an den HNC angeschlossen werden.

Der FC-Anschluss am S-Server erfolgt entweder über einen FC-Switch oder direkt am FC-Kanal des S-Servers.

Mit den zwei eingebauten Kanalanschlüssen (Ports am FC- und/oder ESCON-Controller) kann der HNC am gleichen oder an zwei unterschiedlichen S-Servern angeschlossen werden. Details zu einem auf diese Weise möglichen Redundanzkonzept sind im BCAM-Handbuch [4] beschrieben.

Der HNC kann auch parallel zu einem weiteren HNC oder zu Platten-Systemen am gleichen FC-Kanal des S-Servers angeschlossen werden.

Der HNC unterstützt als Verbindungstyp LOCLAN die Kommunikation zwischen verschiedenen BS2000/OSD-Systemen, die

- im gleichen BS2000-Server laufen
- auf zwei verschiedenen BS2000-Servern laufen die am gleichen HNC angeschlossen sind

Der Datentransfer wird dabei intern im HNC abgewickelt, ohne das Netz zu belasten.

BS2000-Anschlüsse, d.h. Kommunikationsverbindungen zwischen den BS2000/OSD-Systemen und dem LAN werden durch sogenannte virtuelle Netzanschlüsse (in anderen Dokumenten auch als VCAs = Virtual Channel Adapters bezeichnet) hergestellt.

Den Betrieb vieler VMs oder BS2000/OSD-Systeme unterstützt der HNC mit:

- maximal 128 BS2000-Anschlüsse pro Fibre Channel
- maximal 128 BS2000-Anschlüsse im Falle von ESCON (HNC-IV 91853)

Die an einem HNC tatsächlich konfigurierbaren ZASLAN-Anschlüsse hängen von der Anzahl der zur Verfügung stehenden Lizenzen/MAC-Adressen ab.

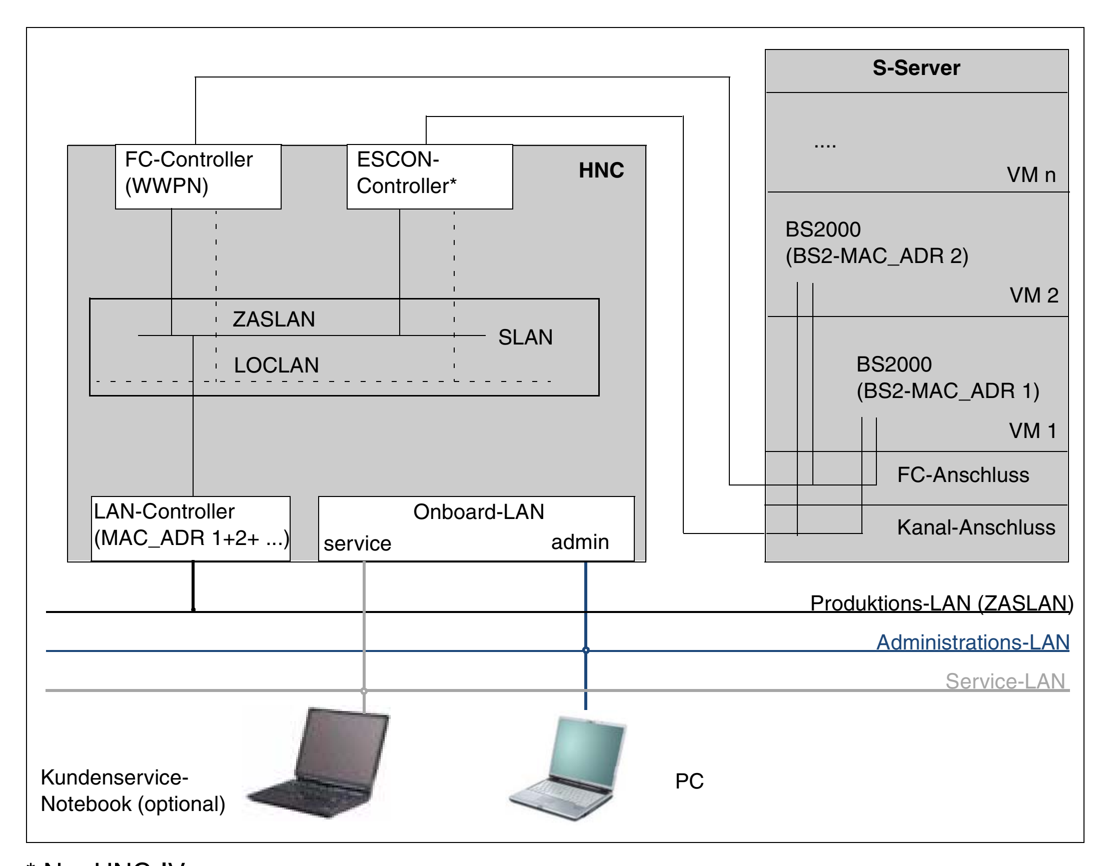
Aus Sicherheitsgründen bietet der HNC bereits in der Basisausführung eigene physikalisch getrennte LAN-Anschlüsse für Administration (Administrations-LAN), für Wartung und Remote Service (Service-LAN) sowie für die Netzanbindung der BS2000-Systeme (BS2000-Anschlüsse vom Typ ZASLAN). Damit ist die Entkopplung der Administrationspfade von den Datentransferpfaden sicher gestellt.

Der HNC-Manager ist die graphische Web-Oberfläche des HNC und bietet folgende Funktionen:

- Detaillierte Anzeige aller BS2000-Anschlüsse einschließlich des aktuellen Status und Möglichkeit des Neustarts einzelner BS2000-Anschlüsse. Die BS2000-Anschlüsse oder VCAs (pro BS2000-Anschluss ein emuliertes Gerätepaar) konfiguriert der Service-Techniker bei der Inbetriebnahme des HNC.
- Anzeige der nötigen Informationen zur Software und Hardware des HNC einschließlich des aktuellen Status
- Verwaltung der Zugangsberechtigungen zum HNC
- Administration des HNC, z.B. LAN-Konfiguration oder NTP
- Wartung des HNC, z.B. Konfigurationsdatensicherung oder Update

2.1 Prinzipielle Arbeitsweise

Folgendes Bild zeigt schematisch die möglichen Anschlüsse des HNC-IV und des HNC-V. Das Bild beschränkt sich auf die für dieses Handbuch relevanten Komponenten und Verbindungen.



* Nur HNC-IV

Der Datentransfer zwischen dem BS2000-System und den angeschlossenen LANs läuft über ein Gerätepaar (WRITE- und READ-Gerät).

Datenpakete werden von einem BS2000-System erzeugt und über einen Kanal (WRITE-Gerät) und die HNC-interne LAN-Komponente SLAN an eines der angeschlossenen LANs gesendet oder sie werden von SLAN (Shared LAN) empfangen und über die Geräteadresse eines Kanals (READ-Gerät) zu einem BS2000-System weitergeleitet (Verbindungstyp ZASLAN).

Das BS2000/OSD-System kann über Fibre Channel (FC) oder über ESCON-Kanal (nur HNC-IV 91853) an den HNC angeschlossen werden. Der FC-Controller ist durch seinen WWPN (World Wide Port Name) eindeutig gekennzeichnet.

Die MAC-Adresse im Kopf des Datenpaketes ist das Kriterium, um empfangene Datenpakete im VM-Betrieb zu den unterschiedlichen BS2000/OSD-Systemen weiterzuleiten. Hierfür können die LAN-Controller Datenpakete mit unterschiedlichen Empfängeradressen empfangen und an unterschiedliche Senderadressen senden.

Am FC- oder ESCON-Anschluss benutzt der HNC zwei Geräteadressen: eine für Read-Befehle und eine für Write-Befehle. Damit ist ein quasi Vollduplex-Betrieb möglich.

Der Geräteadresse wird eine MAC-Adresse zugeordnet. Die transferierten Datenpakete werden im HNC nicht weiter bearbeitet. Zwischen dem BS2000-System und dem HNC läuft kein spezielles Protokoll ab.

Verbindungstyp ZASLAN

Der HNC überträgt im Wesentlichen Datenpakete zwischen BS2000-System und LAN:

- Der LAN-Controller transferiert die Datenpakete in oder aus dem zentralen Speicher des HNC zum LAN.
- Der FC- oder ESCON-Controller führt mit Unterstützung der HNC-CPU den Pakettransfer zwischen Speicher und dem FC- oder ESCON-Anschluss des BS2000-Systems durch.

Verbindungstyp LOCLAN

Als Spezialfall ermöglicht HNC als Verbindungstyp LOCLAN die Kommunikation zwischen verschiedenen BS2000/OSD-Systemen, die

- im gleichen BS2000-Server laufen
- auf zwei verschiedenen BS2000-Servern laufen die am gleichen HNC angeschlossen sind

Diese Kommunikation (das Routing im HNC) wird vom Softwaremodul SLAN (internes „shared LAN“) realisiert. Es stellt Verbindungen zwischen einem BS2000-(Gast-)System und einem LAN am HNC her.

Damit können z.B. Gastsysteme desselben S-Servers über LOCLAN kommunizieren.

2.1.1 LAN-Anbindung des HNC

Der HNC ist zu eigenen Administrations- und Servicezwecken in folgende Netzwerke eingebunden:

Administrations-LAN

Das Administrations-LAN bietet den Zugang zum HNC über einen externen PC. Das Administrations-LAN verwaltet der Administrator über den HNC-Manager.

Service-LAN

Das Service-LAN bietet den Zugang zum HNC über einen externen Service-PC oder direkt über den SKP. Das Service-LAN verwaltet der Kundendienst.

2.1.2 BS2000-Anschlüsse und emulierte BS2000-Geräte

Am HNC können Sie für jeden der beiden Verbindungstypen (ZASLAN oder LOCLAN) mehrere BS2000-Anschlüsse definieren.

Im BS2000/OSD stellen sich diese als emulierte Geräte mit jeweils zugehörigem Gerätepaar (Geräteadresse eines Kanals) dar. Damit die emulierten Geräte im BS2000/OSD bedient werden können, müssen sie dort generiert und zugewiesen werden.

Aus HNC-Sicht werden ZASLAN- und LOCLAN-Anschlüsse nachfolgend zusammenfassend BS2000-Anschlüsse genannt. Für BS2000-Anschlüsse wird in älteren Dokumentationen oft auch die Bezeichnung VCA (Virtual Channel Adapter) benutzt.

In BS2000/OSD werden LAN-Geräte über ihren mnemotechnischen Namen identifiziert und angesprochen. Der mnemotechnische Name wird kurz Mnemonik genannt und in der BS2000-Geräteverwaltung mit MN abgekürzt.

Die BS2000-konforme Geräteadresse wird beim Konfigurieren eines emulierten Geräts im BS2000 festgelegt. Dabei gibt es zwischen BS2000 und HNC Begriffsunterschiede:

- Der HNC kann an den S-Server über Fibre Channel (FC0, FC1) oder ESCON angeschlossen werden. Der entsprechende Channel-Path-Identifier (entspricht einem virtuellen Kanal) wird im BS2000 bei der Systemgenerierung festgelegt.
- Die am HNC vergebene Unit-ID findet sich im BS2000 in der Geräte-Adresse wieder (entspricht der sogenannten Host-LUN).

Zu den Geräteadressen in BS2000/OSD siehe auch das Handbuch „Systeminstallation“ [1].

2.2 Hardware

Die Hardwarebasis des HNC ist ein PRIMERGY-Server der Serie TX300 mit folgender Ausstattung

- Basic Unit
  - 1 DVD-Laufwerk
  - keine lokale Konsole!
- Onboard-LAN
  - 2x GBit LAN onboard
    Die Onboard LAN-Schnittstellen sind für Administration und Service reserviert.
- Mögliche Ausbauten für die Anschlusskarten
  - Für die Kanalanbindung stehen in Summe zwei Kanäle (FC oder ESCON) zur Verfügung.

  Für die Netzanschlüsse an das LAN sind in Summe höchstens vier Anschlüsse zulässig.

Kanal- und LAN-Anschlüsse HNC-V		
Fibre Channel	**91854-KCG (10/100/1000 CU)**	**91854-KGF (1000 Fiber)**
2	2 - 4	0
2	2	1 - 2

Kanal- und LAN-Anschlüsse HNC-IV			
Fibre Channel	**ESCON-Kanal**	**91853-KCG (10/100/1000 CU)**	**91853-KGF (1000 Fiber)**
1 - 2	0	2 - 4	0
1 - 2	0	2	1 - 2
1	1 oder 1 Bündel	2 - 4	0
1	1 oder 1 Bündel	2	1
0	2 oder 1 Bündel	2 -4	0
0	2 oder 1 Bündel	2	1

Beim Anschluss des HNC über zwei ESCON-Kanäle an den gleichen BS2000/OSD-Server können die beiden Kanäle auch als Bündel betrieben werden. Dies dient der Optimierung des Kanaldurchsatzes und der Ausfallsicherheit.

- Anbindung an den Remote Service

  Beim HNC-V 91854 wird der Remote Service-Zugang durch die Anbindung an das Service-LAN hergestellt. Der HNC-IV 91853 kann über eine serielle V24-Verbindung an einen SKP 3970 angeschlossen werden. Optional kann der HNC-IV 91853 auch mit dem Service-LAN verbunden werden.

  Über diese Anschlüsse können Verbindungen vom SKP zum HNC hergestellt werden, die auch über Remote-Service (am SKP) benutzt werden können. Auf diese Weise ist der HNC in die Remote Service-Infrastruktur von Fujitsu Technology Solutions eingebunden.

Aufbau-Varianten

Der HNC wird als Floor-Stand und auch als Rack-Einschub angeboten.

2.3 Software

Dieses Handbuch beschreibt den Software-Stand V2.0 für den HNC-V 91854. Dieser Software-Stand kann auch auf HNC-IV 91853 eingesetzt werden. Nur die HNC-IV 91853 Hardware unterstützt ESCON.

Die HNC-Software ist Linux-basiert. Sie sehen unter anderem die Version der Linux-Systembasis SLES 10 SP3 mit Security-Korrekturen, z.B. bei der Pflege des Systems (Security Fixes).

Ein SNMP-Agent, der auch Traps unterstützt, ist vorinstalliert. Der SNMP-Agent unterstützt folgende MIBs:

- RFC 1213 (MIB-II),
- MIBs mit privaten Traps, siehe „SNMP konfigurieren“ auf Seite 43

Wenn Sie im HNC-Manager *HNC Management* wählen, sehen Sie in der Registerkarte *Systemübersicht* unter anderem die Linux-Version und den Stand bezüglich der Security Fixes.

Für die Produkte auf BS2000-Ebene gelten folgende Software-Voraussetzungen:

- BS2000/OSD ab V5.0
- openNet Server ab V3.1 (Unterstützung von Fibre Channel)
- für VLAN openNet Server ab V3.2
- für Link Aggregation & Checksum Offloading openNet Server ab V3.4

In der Registerkarte *HNC Management>Systemübersicht* zeigt der HNC relevante Informationen zur installierten Software, siehe hierzu auch „Informationen über den HNC einholen“ auf Seite 39.

3 HNC bedienen

Sie bedienen den HNC mit dem HNC-Manager oder direkt über die CLI (Command Line Interface). Der HNC-Manager ist eine Web-Anwendung mit GUI (Graphical User Interface), die folgende Funktionen bietet:

- Anzeige und Neustart von BS2000-Anschlüssen, siehe „BS2000-Anschlüsse“ auf Seite 33
- Einrichten und Ändern personalisierter Administrator-Kennungen, siehe „Kennungen verwalten“ auf Seite 46
- Anzeige und Änderung der HNC-Konfiguration, siehe „HNC konfigurieren“ auf Seite 41
- Wartung des HNC, siehe „Diagnose und Wartung“ auf Seite 53
- Zugang zum HNC über CLI, siehe „Zugang zum CLI“ auf Seite 31

Der HNC wird vor Auslieferung nach Ihren Anforderungen installiert und konfiguriert.

3.1 HNC-Manager

Um den HNC-Manager „remote“ von einem PC aus zu nutzen, brauchen Sie einen PC mit Netzwerkverbindung zum HNC, installierter Java Runtime Environment ab Version 1.6.x und installiertem Browser. Der Microsoft Internet Explorer ab Version 7.0 sowie Mozilla Firefox ab Version 3.0 werden unterstützt.

Folgende Voraussetzungen muss der Browser auf Ihrem PC erfüllen:

- Die Ausführung von Applets ist zugelassen.
- Die Ausführung von JavaScript ist zugelassen.
- Cookies sind zugelassen.

Ein Terminal-Zugang (Shell zum HNC) ist in den HNC-Manager eingebettet.

Die Kommunikation erfolgt grundsätzlich über HTTPS (HyperText Transfer Protocol Secure), wobei die darunter liegenden Verschlüsselungsprotokolle SSL 3.0 (Secure Sockets Layer) und TLS 1.0 (Transport Layer Security) unterstützt werden. SSL 2.0 wird nicht unterstützt. Für HTTP-Aufrufe findet eine automatische Umlenkung nach HTTPS statt.

Die Nutzung von HTTPS/SSL setzt am HNC außer einem SSL-Schlüsselpaar auch ein sogenanntes (digitales) SSL-Zertifikat voraus. Zu den Sicherheitsaspekten beim Nutzen des HNC-Managers siehe das Sicherheitshandbuch [6].

Die Sprachen des HNC-Managers sind Deutsch und Englisch. Die Sprache können Sie durch die Sprachoption im Kopfbereich einstellen.

3.1.1 HNC-Manager aufrufen

- ► Geben Sie die Adresse des HNC in die Adressleiste des Browsers ein.
- ► Drücken Sie die ↵-Taste. Das Anmeldefenster öffnet sich.

3.1.2 Anmelden

Der Zugang zum HNC-Manager ist geschützt. Sie müssen sich mit Ihrer Kennung und dem zugehörigen gültigen Passwort anmelden.

Das Anmeldefenster bildet den Zugang zum HNC-Manager. Es unterscheidet sich im Aufbau von den sonstigen Fenstern:

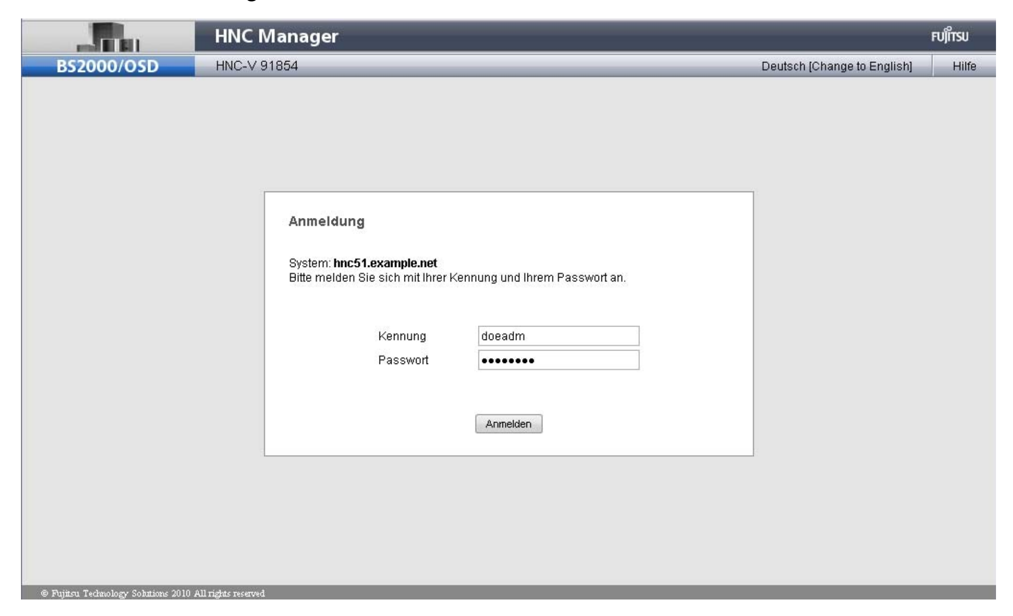
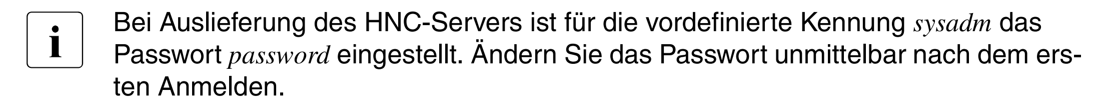


Bild 1: Anmeldefenster HNC-Manager

So melden Sie sich am HNC-Manager an:

► Geben Sie Ihre Kennung ein.

► Geben Sie Ihr Passwort ein.



Bei Auslieferung des HNC-Servers ist für die vordefinierte Kennung *sysadm* das Passwort *password* eingestellt. Ändern Sie das Passwort unmittelbar nach dem ersten Anmelden.

Es öffnet sich die Seite *BS2000-Anschlüsse* mit der Übersicht über alle BS2000-Anschlüsse als Startseite.

Das Anmeldefenster wird auch zum erneuten Anmelden ausgegeben, wenn Sie sich abgemeldet haben oder die Session wegen Inaktivität abgebrochen wurde (siehe „Session-Verwaltung“ auf Seite 21).

3.1.3 Abmelden

So melden Sie sich vom HNC-Manager ab:

► Klicken Sie *Abmelden* (Kopfbereich des Hauptfensters).
Siehe „Hauptfenster“ auf Seite 23.

3.1.4 Session-Verwaltung

Beim Anmelden am HNC-Manager wird eine Session mit einer eindeutiger Session-ID aufgebaut. Alle Anfragen mit der gleichen Session-ID betrachtet der HNC als zusammenhängend und ordnet sie Ihrer Kennung zu.

Über *Abmelden* im Kopfbereich des Hauptfensters beenden Sie die aktuelle Session explizit. Ohne explizites Abmelden läuft die Session ab, wenn Sie 20 Minuten inaktiv sind, das heißt wenn der HNC-Manager in dieser Zeit keine Aktion registriert.

Wenn Sie bei abgelaufener Session eine Funktion wählen, öffnet sich das Anmeldefenster und Sie müssen sich neu anmelden.

Wenn Sie bei abgelaufener Session eine Aktion im Arbeitsbereich starten, öffnet sich ein Dialog mit der Meldung:

Die Aktion konnte nicht ausgeführt werden. Ihre Session ist abgelaufen. Melden Sie sich bitte neu an.

Nach Schließen des Dialogs öffnet sich das Anmeldefenster. Siehe „Dialoge“ auf Seite 25.

3.1.5 Oberfläche des HNC-Managers

Die folgenden Abschnitte beschreiben die Oberfläche des HNC-Managers und führen Begriffe ein, die im Handbuch und in der Online-Hilfe verwendet werden.

3.1.5.1 Fenster-Typen

Im HNC-Manager gibt es verschiedene Fenster-Typen:

- Das Anmeldefenster: Fenster, in dem Sie sich mit Kennung und Passwort anmelden. Siehe „Anmelden“ auf Seite 20
- Das Hauptfenster: Fenster, das zwischen An- und Abmeldung am HNC-Manager immer sichtbar ist; es enthält die Navigationselemente und den Arbeitsbereich, in dem Informationen ausgegeben und Aktionen angestoßen werden.
- Dialog: Fenster, das sich beim Starten einer Aktion öffnet und nach Abschluss der Aktion wieder geschlossen wird. Es dient auch zur Ausgabe von Fehlermeldungen.
- Das Fenster der Online-Hilfe: Fenster, das sich beim Aufrufen der Online-Hilfe öffnet. Siehe „Online-Hilfe aufrufen“ auf Seite 28.

3.1.5.2 Hauptfenster

Das Hauptfenster des HNC-Managers öffnet sich, sobald Sie sich am HNC-Manager angemeldet haben. Es besteht aus folgende Bereichen:

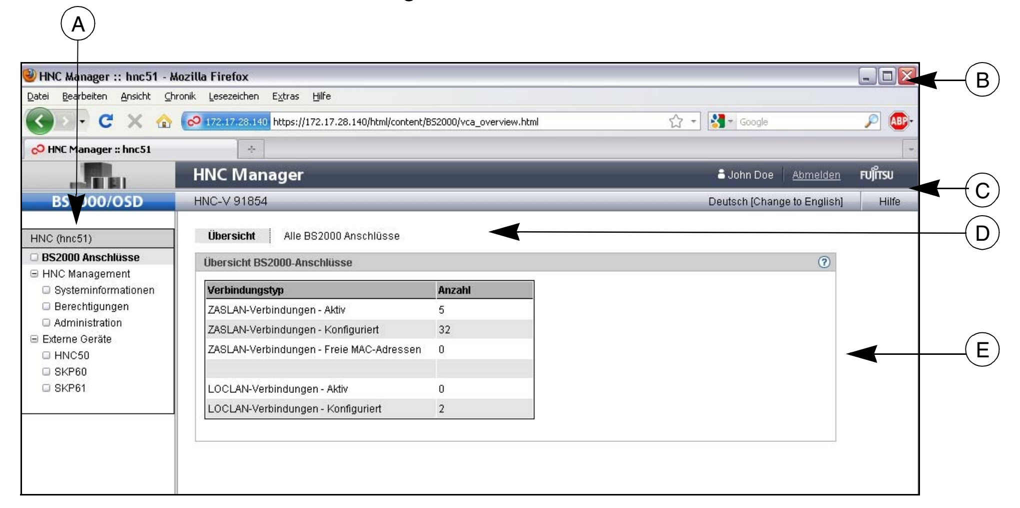


Bild 2: HNC-Manager: Bereiche im Hauptfenster

	Bereich	Bedeutung
A	Primärnavigation	Auswahl eines Objektes oder einer Funktion
B	Titelzeile	Zeigt neben der Bezeichnung *HNC-Manager* den FQDN=Name des Systems (Fully Qualified Domain Name)
C	Kopfbereich	Zeigt allgemeine Informationen, Sprachoptionen, Hilfe, Abmelden
D	Sekundärnavigation	Auswahl einer Registerkarte zum gewählten Objekt oder Funktion
E	Arbeitsbereich	Der Arbeitsbereich kann mehrere Gruppen enthalten. Jede Gruppe ist optisch mit einem Rahmen zusammengefasst und mit einer Überschrift versehen: – Daten ausgeben (in der Regel in Tabellenform) – Aktionen anstoßen, um Aufgaben zur Verwaltung des HNC auszuführen. Symbole und Schaltflächen lösen Aktionen aus.

Elemente des Hauptfensters

Die folgenden Grafiken zeigen anhand des Beispiels „Konfigurationsdaten-Sicherung“ wichtige Elemente des HNC-Managers. Die nummerierten Elemente der Grafik werden in der nachfolgenden Tabelle aufgelistet und bezeichnet.

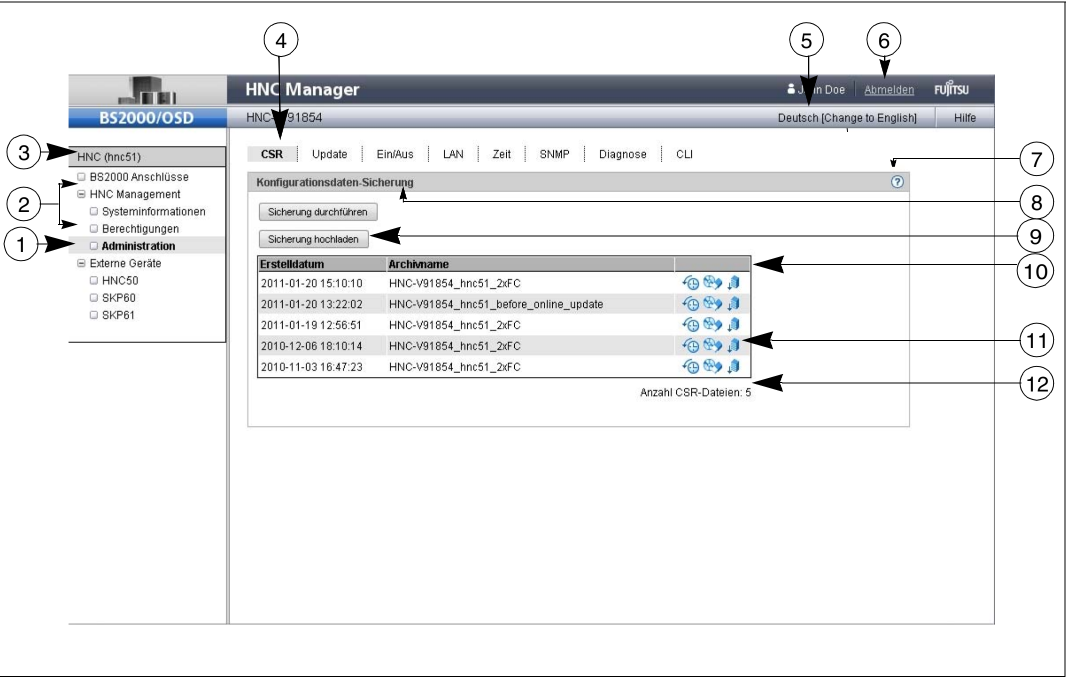
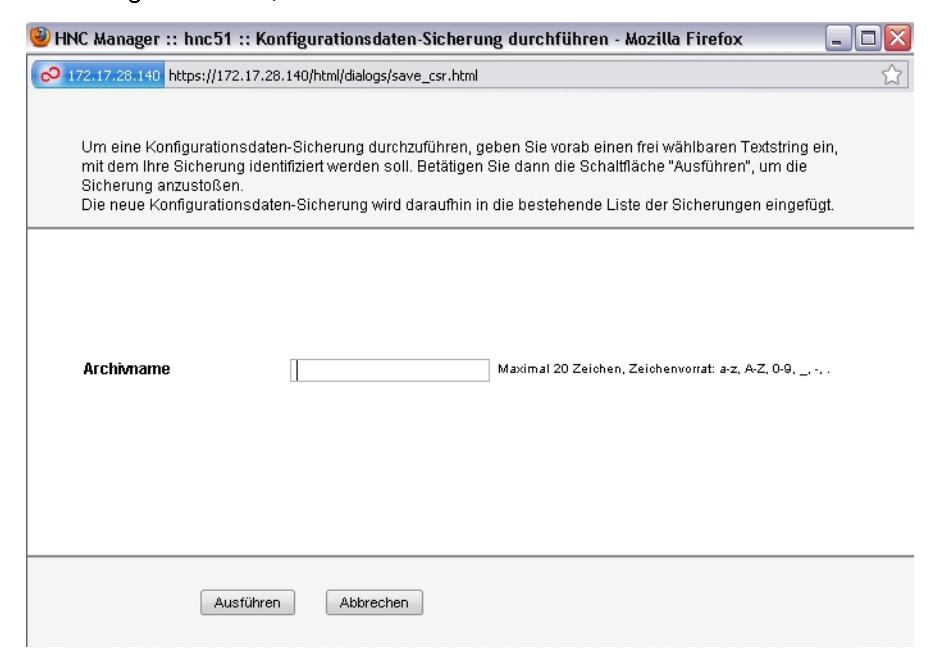


Bild 3: HNC-Manager: Elemente des Hauptfensters

Position	Bedeutung
1	Ausgewählte Funktion der Primärnavigation
2	Objekte und Funktionen
3	Vom Administrator vergebener Name des HNC
4	Aktive Registerkarte der Sekundärnavigation
5	Sprachoption (Deutsch/Englisch)
6	Anmelde-Information: Personenbezogener Name oder Kennung (rot, falls das Passwort bald ungültig wird)
7	Symbol zum kontextsensitiven Aufruf der Online-Hilfe (siehe „Online-Hilfe aufrufen“ auf Seite 28)
8	Gruppentitel
9	Beschriftete Schaltfläche
10	Tabelle mit Eigenschaften der ausgegebenen Objekte
11	Symbole zum Auslösen von Aktionen
12	Tabellen-Information: Anzahl Objekte

3.1.5.3 Dialoge

Ein Dialog öffnet sich, sobald Sie eine Aktion starten:



Ein Dialog besteht aus:

- Titelzeile mit folgenden Informationen:

  HNC-Manager:: FQDN:: Aufgabe
  FQDN=Name des Systems (Fully Qualified Domain Name)
  Aufgabe=Auszuführende Aktion

- Kopfbereich: Informationen zur Aktion
- Optionen (optional): Felder zur Eingabe oder Auswahl von Parameterwerten. Mögliche Werte, maximale Zeichenlänge und die verwendbaren Zeichen sind neben den Feldern erklärt.
- Bereich mit beschrifteten Schaltflächen, z.B. *Ausführen* und *Abbrechen*.

In einem einfachen Dialog ohne Optionen bestätigen Sie lediglich die aufgerufene Aktion. Alternativ können Sie die Aktion auch abbrechen.

Oft geben Sie jedoch für die Optionen Werte ein oder bestätigen vorgegebene Werte. Erst nach Eingabe oder Auswahl aller Werte führen Sie die Aktion aus (oder brechen Sie ab).

Der HNC-Manager überprüft Ihre Eingabe und reagiert auf unzulässige oder fehlende Eingaben mit Fehlermeldungen oder markiert die fehlerhafte Option. Auch die erfolgreiche Ausführung der Aktion meldet der HNC-Manager im Dialog. Nach der Ausführung einer Aktion schließen Sie den Dialog mit *Schließen* und aktualisieren damit das Hauptfenster.



Ein zusätzliches Fenster im Vordergrund, z.B. einen Dialog, müssen Sie immer über seine beschriftete Schaltfläche schließen, um das Hauptfenster zu aktualisieren.

3.1.6 Objekt oder Funktion aufrufen

So rufen Sie im HNC-Manager ein Objekt oder eine Funktion auf:

► Wählen Sie mit Mausklick ein Objekt oder eine Funktion aus der Primärnavigation.

Eine oder mehrere zugehörige Registerkarten öffnen sich. Im Arbeitsbereich werden für die erste Registerkarte die relevanten Informationen in ein oder mehreren Tabellen angezeigt. Außerdem können Sie gegebenenfalls mit Schaltflächen oder Symbolen Aktionen ausführen.

► Wählen Sie mit Mausklick gegebenenfalls eine andere Registerkarte.

Bei Auswahl einer anderen Registerkarte ändert sich der Inhalt des Arbeitsbereichs.

Das gewählte Objekt und die gewählte Registerkarte werden fett und schwarz auf weißem Hintergrund hervorgehoben.

Beispiel

HNC Management > Administration, Registerkarte *CSR*.
HNC Management > Administration entspricht einer Auswahl in der Primärnavigation, *CSR* einer Auswahl in der Sekundärnavigation, auch Registerkarte genannt.

Wenn keine Daten vorhanden sind, wird im Arbeitsbereich eine leere Tabelle ausgegeben.

3.1.7 Navigieren

Sie wechseln beliebig zwischen den Objekten und Funktionen durch Klicken. Zum Vor- und Zurück-Navigieren und Aktualisieren des Hauptfensters können Sie auch die Browser-Funktionen nutzen.

Manche Funktionen des HNC-Managers öffnen ein neues Browser-Fenster oder eine neue Browser-Registerkarte:

- Aufruf der Online-Hilfe
- Aufruf der Terminal-Fenster für das CLI
- Öffnen eines Dialogs

3.1.8 Tabelle filtern

Filter erleichtern die Handhabung von umfangreichen Tabellen.

In bereits angezeigten Tabellen können Sie mit Freitext- und Auswahlmenü-Filtern in Tabellenspalten die aktuell angezeigten Daten einschränken.

3.1.9 Tabelle sortieren

So sortieren Sie eine Tabelle:

► Fahren Sie mit dem Mauszeiger über die Spaltenüberschriften der Tabelle.
Wenn der Mauszeiger zu einer symbolischen Hand wird, können Sie die Tabelle nach den Werten dieser Spalte sortieren.

► Klicken Sie auf die Spaltenüberschrift.

Die Tabelle wird sortiert.

Wenn Sie wiederholt auf dieselbe Spaltenüberschrift klicken, ändert sich die Sortierung von aufsteigend zu absteigend und umgekehrt.
Eine Sortierung nach einer anderen Spalte hebt die bisherige Sortierung auf.

Eine Sortierung bleibt bis zum nächsten Aufbau des Hauptfensters sichtbar.

3.1.10 Online-Hilfe aufrufen

Der HNC-Manager verfügt über eine integrierte kontext-sensitive Online-Hilfe.

Die Online-Hilfe enthält Informationen zur gesamten Oberfläche des HNC-Managers.

Es gibt zwei Wege die Online-Hilfe aufzurufen:

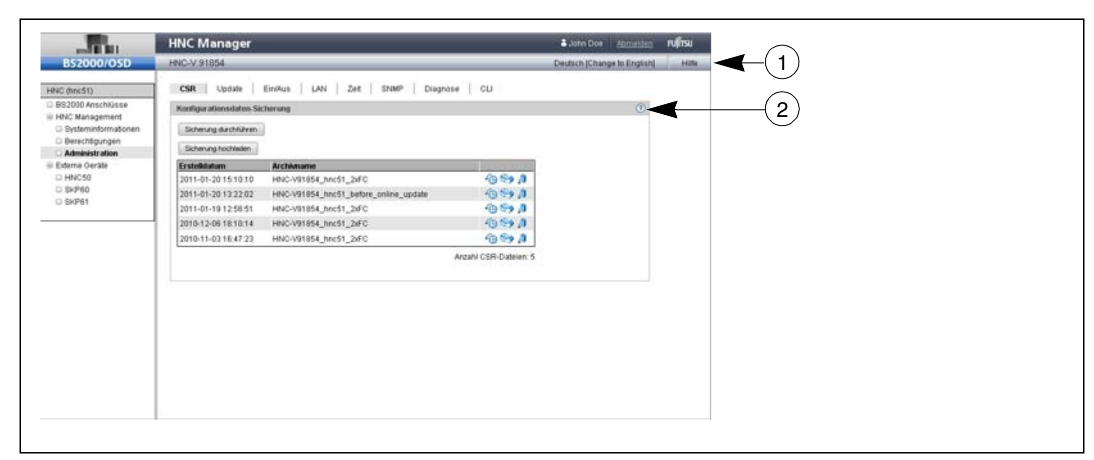


Bild 4: Online-Hilfe aufrufen

Position	Funktion
1	Funktion *Hilfe* im Kopfbereich des HNC-Managers: Die Startseite der Online-Hilfe wird in einem neuen Browser-Fenster aufgerufen.
2	*Hilfe*-Symbol im Arbeitsbereich: Der passende Abschnitt der Online-Hilfe (themenspezifisch) wird in einem neuen Browser-Fenster geöffnet. Sie erhalten Informationen zur Funktionalität des aktuellen Fensters.

Folgendes Bild zeigt die Startseite der Online-Hilfe:

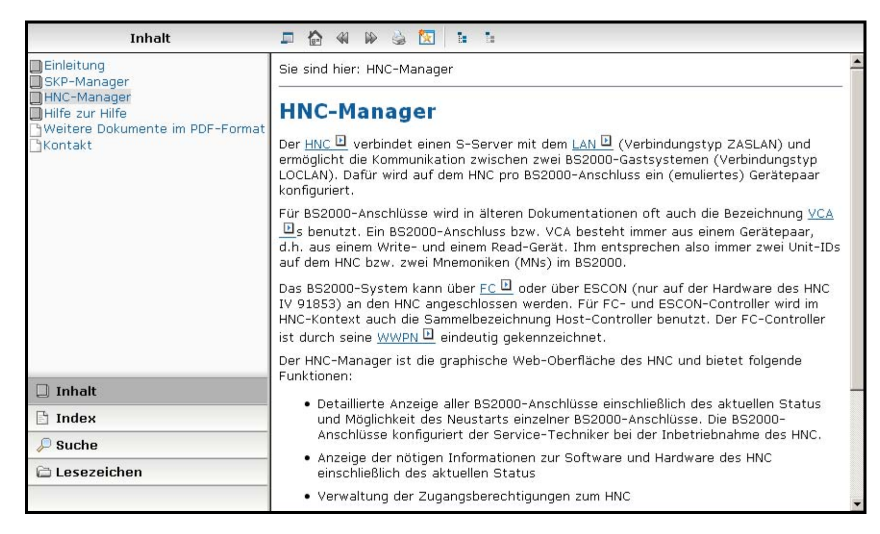


Bild 5: Startseite der Online-Hilfe

Links sehen Sie das Inhaltsverzeichnis, das analog zur Primär- und Sekundärnavigation des HNC-Managers aufgebaut ist. Rechts werden die ausgewählten Inhalte angezeigt. Die angezeigten Inhalte können Sie drucken (Drucker-Symbol) und zur Favoritenliste hinzufügen (Stern-Symbol).

Sie können die Navigation ein- und ausklappen, um den Inhaltsbereich zu vergrößern. Anstelle des Inhaltsverzeichnisses können Sie auch navigieren über

– das Stichwortverzeichnis (Index)

– die Suchmaske

– Ihre persönlichen Favoriten

Klicken Sie zur Auswahl ein Register unter der Navigation.

Sie können innerhalb der kompletten Online-Hilfe navigieren und suchen, unabhängig davon, wie Sie sie aufgerufen haben.

3.1.11 Fehlerbehandlung

Mögliche Probleme können sein:

– Sie können keine Verbindung aufbauen.

– Sie können eine Aktion nicht starten.

– Während einer Aktion treten Fehler auf.

– Die Verbindung wird unterbrochen.

Wenn Sie keine Verbindung aufbauen können, prüfen Sie die eingegebene Adresse und die Erreichbarkeit und gegebenenfalls den Systemstatus des HNC.

Wenn die Durchführung einer Aktion scheitert, wird die Ursache als Fehlermeldung im Parameterbereich des Dialogs angegeben.

Bei manchen Aktionen, z.B. einem HNC-Neustart, wird die Verbindung unterbrochen. Sie müssen sich anschließend neu anmelden.

Rufen Sie die Online-Hilfe themenspezifisch auf, wenn Sie weitere Informationen benötigen (siehe „Online-Hilfe aufrufen“ auf Seite 28).

Wenn Sie das Problem dennoch nicht lösen können, setzen Sie sich mit Ihrem Service in Verbindung.

3.2 Zugang zum CLI

Der HNC-Manager bietet den Zugang zum CLI (**C**ommand **L**ine **I**nterface) als Funktion an. Bei Aufruf wird in einem Terminal die Linux-Shell zur Eingabe der Kommandos aufgerufen.

Alternativ können Sie die Shell auch unabhängig vom HNC-Manager über einen SSH-Client (z.B. PuTTY) aufrufen, siehe das Sicherheitshandbuch [6].

Sie öffnen die Shell unter der Kennung, mit der Sie am HNC angemeldet sind. Das Kommando `cli_info` informiert jeweils über den verfügbaren Funktionsumfang. Eine detaillierte Beschreibung der Kommandos können Sie über die Online-Hilfe aufrufen.

> **i** Unter den Kennungen sollten Sie im Linux keine größeren Datenmengen dauerhaft ablegen, da ansonsten das System beeinträchtigt werden könnte.

3.2.1 Terminal-Fenster öffnen

► Wählen Sie *HNC Management > Administration > CLI*.



► Wählen Sie die gewünschte Bildschirmgröße und klicken Sie *öffnen*.

Das Terminal-Fenster öffnet sich und fordert Sie zur Eingabe des Passworts für die Kennung auf, unter der Sie am HNC-Manager arbeiten.

► Geben Sie das Passwort ein und drücken Sie die ↵-Taste.

3.2.2 Terminal-Fenster schließen

► Geben Sie das Kommando *exit* ein, um das Terminal-Fenster zu schließen.

3.2.3 Kommandos

Beim CLI-Zugang stehen Ihnen Kommandos zur Verfügung, die nachfolgend kurz beschrieben werden.

Die Anwendung von diesen Linux-Kommandos sowie der Shell wird als bekannt vorausgesetzt und hier nicht näher beschrieben. Detaillierte Informationen zu den Kommandos erhalten Sie in der Online-Hilfe zum HNC-Manager.

3.2.3.1 auditLog

Das Kommando *auditLog* verwaltet die Protokolldateien der Auditlog-Funktion, die jede Aktion (Konfigurations- oder Zustandsänderung) protokolliert, die am HNC über die Web-Oberfläche oder über ein CLI-Kommando ausgeführt wird. Das Kommando listet die Protokolldateien auf oder gibt sie aus.

Der Aufruf des Kommandos lautet allgemein:

```
auditLog <option> [<operand>…]
```

3.2.3.2 cli_info

Das Kommando *cli_info* zeigt die am CLI verfügbaren Kommandos.

Der Aufruf des Kommandos lautet:

```
cli_info
```

3.2.3.3 init

Das Kommando *init* fährt den HNC herunter und schaltet ihn aus oder führt einen Reboot durch.

Der Aufruf des Kommandos lautet:

```
init <operand>
```

4 BS2000-Anschlüsse

Die zentrale Aufgabe des HNC besteht in der Anzeige der BS2000-Anschlüsse und gegebenenfalls einem Neustart eines fehlerhaften Anschlusses. Die Registerkarte *Alle BS2000-Anschlüsse* des HNC-Managers zeigt eine Übersicht aller konfigurierten BS2000-Anschlüsse. Jeden Anschluss können Sie im Zweifelsfall nach Rückfrage neu starten.

Der Software-Stand V2.0 des HNC läuft auf der Hardware des HNC-IV und HNC-V. Der HNC-V nutzt Fibre Channel für die Anschlüsse ans BS2000.

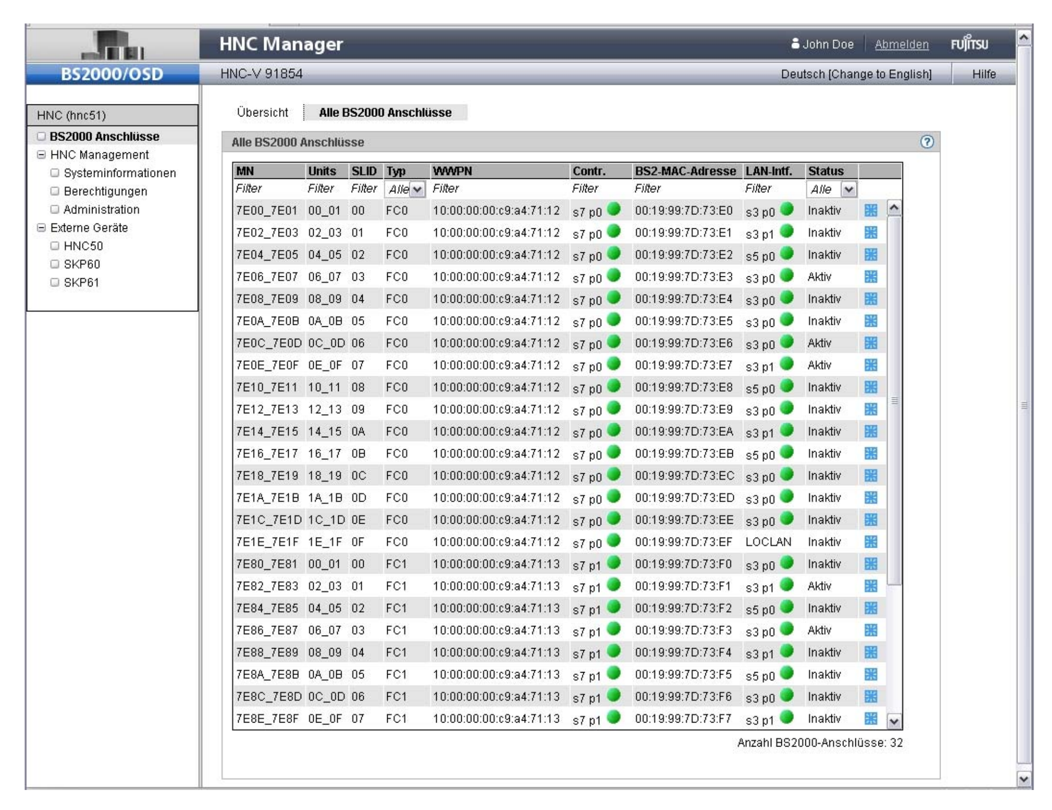
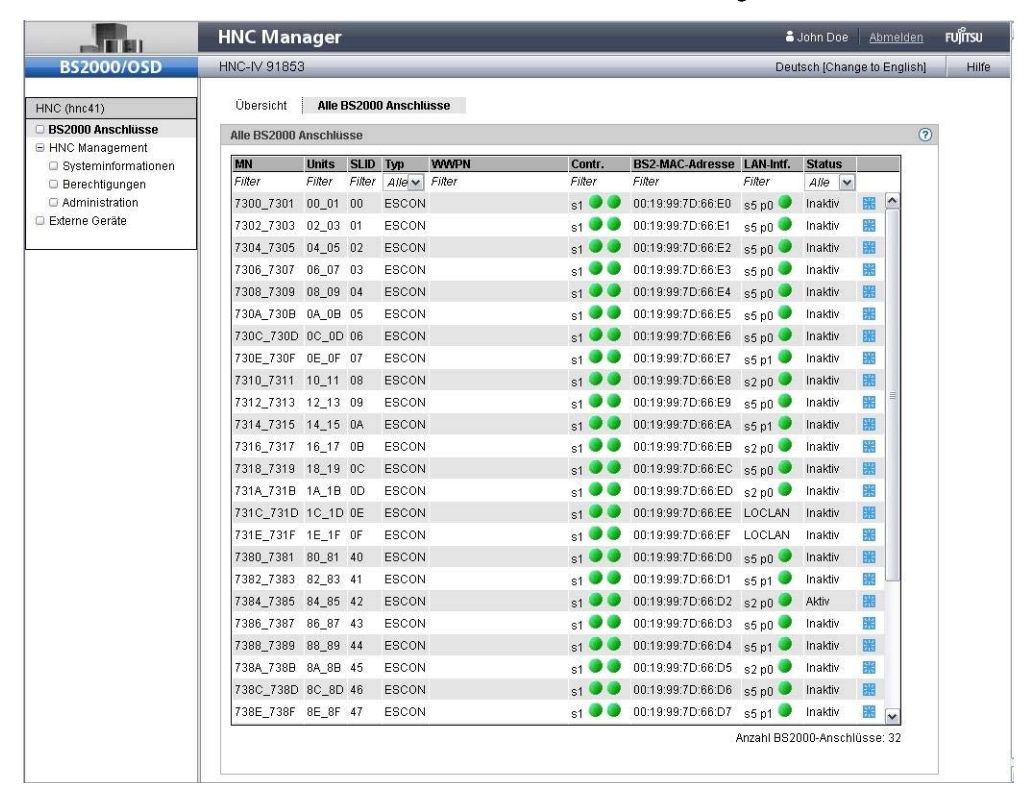


Bild 6: Übersicht der BS2000-Anschlüsse über Fiber Channel (HNC-V)

Mit der HNC-IV Hardware können auch ESCON-Anschlüsse genutzt werden.



MN	Units	SLID	Typ	WWPN	Contr.	BS2-MAC-Adresse	LAN-Intf.	Status
Filter	Filter	Filter	Alle	Filter	Filter	Filter	Filter	Alle
7300_7301	00_01	00	ESCON		s1	00:19:99:7D:66:E0	s5 p0	Inaktiv
7302_7303	02_03	01	ESCON		s1	00:19:99:7D:66:E1	s5 p0	Inaktiv
7304_7305	04_05	02	ESCON		s1	00:19:99:7D:66:E2	s5 p0	Inaktiv
7306_7307	06_07	03	ESCON		s1	00:19:99:7D:66:E3	s5 p0	Inaktiv
7308_7309	08_09	04	ESCON		s1	00:19:99:7D:66:E4	s5 p0	Inaktiv
730A_730B	0A_0B	05	ESCON		s1	00:19:99:7D:66:E5	s5 p0	Inaktiv
730C_730D	0C_0D	06	ESCON		s1	00:19:99:7D:66:E6	s5 p0	Inaktiv
730E_730F	0E_0F	07	ESCON		s1	00:19:99:7D:66:E7	s5 p1	Inaktiv
7310_7311	10_11	08	ESCON		s1	00:19:99:7D:66:E8	s2 p0	Inaktiv
7312_7313	12_13	09	ESCON		s1	00:19:99:7D:66:E9	s5 p0	Inaktiv
7314_7315	14_15	0A	ESCON		s1	00:19:99:7D:66:EA	s5 p1	Inaktiv
7316_7317	16_17	0B	ESCON		s1	00:19:99:7D:66:EB	s2 p0	Inaktiv
7318_7319	18_19	0C	ESCON		s1	00:19:99:7D:66:EC	s5 p0	Inaktiv
731A_731B	1A_1B	0D	ESCON		s1	00:19:99:7D:66:ED	s2 p0	Inaktiv
731C_731D	1C_1D	0E	ESCON		s1	00:19:99:7D:66:EE	LOCLAN	Inaktiv
731E_731F	1E_1F	0F	ESCON		s1	00:19:99:7D:66:EF	LOCLAN	Inaktiv
7380_7381	80_81	40	ESCON		s1	00:19:99:7D:66:D0	s5 p0	Inaktiv
7382_7383	82_83	41	ESCON		s1	00:19:99:7D:66:D1	s5 p1	Inaktiv
7384_7385	84_85	42	ESCON		s1	00:19:99:7D:66:D2	s2 p0	Aktiv
7386_7387	86_87	43	ESCON		s1	00:19:99:7D:66:D3	s5 p0	Inaktiv
7388_7389	88_89	44	ESCON		s1	00:19:99:7D:66:D4	s5 p1	Inaktiv
738A_738B	8A_8B	45	ESCON		s1	00:19:99:7D:66:D5	s2 p0	Inaktiv
738C_738D	8C_8D	46	ESCON		s1	00:19:99:7D:66:D6	s5 p0	Inaktiv
738E_738F	8E_8F	47	ESCON		s1	00:19:99:7D:66:D7	s5 p1	Inaktiv

Bild 7: Übersicht der BS2000-Anschlüsse über ESCON (HNC-IV)

Das folgende Bild zeigt einen HNC im sogenanntem Mischbetrieb (nur am HNC-IV 91853), bei dem die BS2000-Anschlüsse sowohl über ESCON als auch über Fibre Channel realisiert sind.

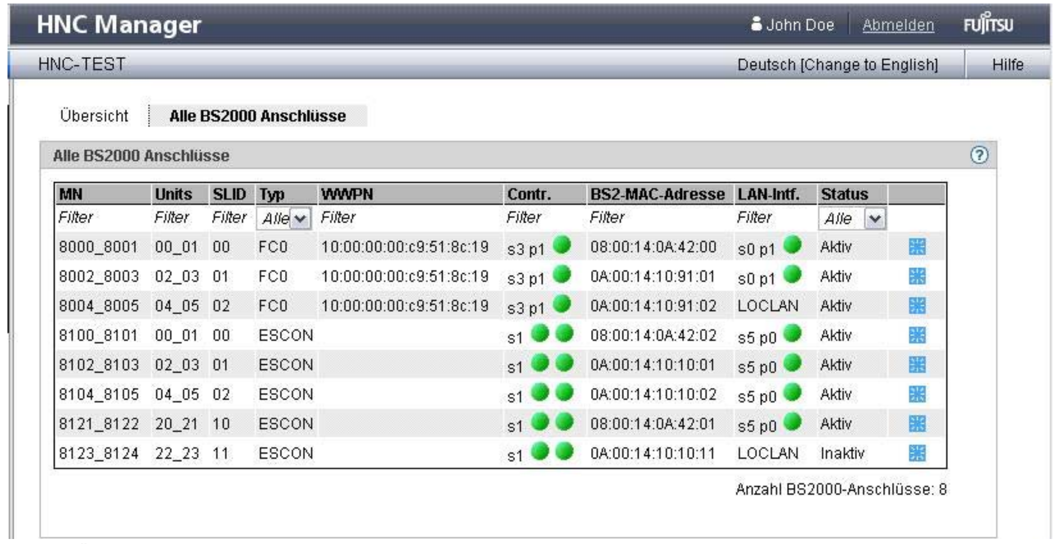


Bild 8: Übersicht der BS2000-Anschlüsse im Mischbetrieb (HNC-IV)

Die Übersicht über die BS2000-Anschlüsse zeigt

- die im BS2000 relevanten Anschlussdaten (z.B. MNs, Units, BS2000-MAC-Adressen)
- Hardware-Informationen zu den LAN-Schnittstellen (Steckplätze und Status als Symbol mit Tooltip)
- Hardware-Informationen zu den Host-Controllern (Steckplätze und Status als Symbol mit Tooltip, WWPN für Fibre Channel)
- Geräte-Emulation - Status Aktiv/Inaktiv/Gestoppt

Am HNC gibt es LOCLAN- und ZASLAN-Anschlüsse. Diese Anschlüsse stellen sich aus BS2000-Sicht als emulierte BS2000-Geräte dar. Die BS2000-Anschlüsse legt ein Service-Techniker bei Inbetriebnahme des HNC an.

Ein BS2000-Anschluss besteht aus einem Gerätepaar, d.h. aus einem Write- und einem Read-Gerät. Ein Anschluss hat deswegen immer zwei Unit-IDs am HNC und zwei BS2000 Mnemoniks im BS2000.

Die Zuordnung der BS2000-MNs beim Konfigurieren der Anschlüsse ist optional und hat nur Dokumentationscharakter. Somit liegt kein Fehler vor oder es hat keine Auswirkungen auf den laufenden Betrieb, wenn keine BS2000-MNs zugewiesen werden. Sie können (durch den Service) auch im Nachhinein im laufenden Betrieb konfiguriert werden.

WWPN und virtuelle WWPN

Jedem Fibre Channel-Anschluss ist ein eindeutiger WWPN (World Wide Port Name) zugeordnet, die den Anschluss identifiziert. Wenn Sie die Hardware für einen Fibre Channel-Anschluss austauschen lassen und wenn der alte FC-Controller sicher nicht mehr benutzt werden soll, können Sie den alten WWPN als virtuellen WWPN weiter nutzen. Sprechen Sie dazu beim Hardware-Tausch das konkrete Vorgehen mit dem Service ab.

Anschlüsse im BS2000 einrichten

Das Gerätepaar eines ZASLAN- oder LOCLAN-Anschlusses muss im BS2000-System generiert werden. Dies kann statisch über die IOCF-Datei (siehe Handbuch „Systeminstallation“ [1]) oder im laufenden Betrieb für die laufende BS2000-Sitzung mit /ADD-IO-UNIT (siehe Handbuch „Kommandos“ [5]) durchgeführt werden. Für die Unit-IDs, die das ZASLAN- oder LOCLAN-Gerät realisieren, werden dabei BS2000-MNs definiert. Im nachfolgenden Beispiel sind die MNs als <mn1> und <mn2> bezeichnet.

Die Kommunikationsgeräte müssen im VM2000-Betrieb dem jeweiligen Gastsystem exklusiv zugeordnet werden (ggf. Eintrag in der RUN-Datei zum Starten der VM), siehe Handbuch „VM2000“ [3]: /ADD-VM-DEVICES UNITS=(<mn1>,<mn2>), VM-ID=<vm-id>

In dem jeweiligen Gastsystem oder im Native-BS2000-System müssen die Geräte zugeschaltet werden (siehe Handbuch „Kommandos“ [5]):
/ATTACH-DEVICE UNIT=(<mn1>,<mn2>)<

Weiterhin müssen die Kommunikationsgeräte sowie die IP-Adressen dem BCAM des jeweiligen BS2000-Systems bekannt gegeben werden. Dies geschieht in der BCAM SOF-Datei (Start Option File) oder auch über Kommandos an der Konsole
(siehe Handbuch „BCAM“ [4]).

Beispiel einer SOF-Datei

Im Gastsystem `LBSVM1` werden 2 redundante Leitungen (`HNCLINE1` und `HNCLINE2`) und das das Gastsystem `LBSVM2` definiert.

```
/DCOPT HOST=LBSVM1,...
/BCOPTION ARP=QUIET,BROADCAST=ON,ISO9542=OFF,SLOW-POLL=ON
/CREATE-NODE NODE-NAME=HNC#NODE,IP-SUBNET-MASK=255.255.255.128

/CREATE-LINE LINE-NAME=HNCLINE1, IP-ADDRESS=172.25.226.242,-
/  L2-PROTOCOL=*CSMACD(NODE-NAME=HNC#NODE,-
/  WRITE-DEVICE=751C,READ-DEVICE=751D, MAX-LPDU-SIZE=*BY-DEVICE,-
/  SLOW-POLL=*ON,AUTO-ROUTE-SWITCHING=*OFF,ROUTE-RESWITCHING=*OFF)
/CREATE-LINE LINE-NAME=HNCLINE2, IP-ADDRESS=172.25.226.252,-
/  L2-PROTOCOL=*CSMACD(NODE-NAME=HNC#NODE,-
/  WRITE-DEVICE=711C,READ-DEVICE=711D, MAX-LPDU-SIZE=*BY-DEVICE,-
/  SLOW-POLL=*ON,AUTO-ROUTE-SWITCHING=*OFF,ROUTE-RESWITCHING=*OFF)

/ACTIVATE-LINE LINE-NAME=HNCLINE1
/ACTIVATE-LINE LINE-NAME=HNCLINE2
/CREATE-PROCESSOR PROC-NAME=LBSVM2,MAX-TSDU-SIZE=65530
/CREATE-ROUTE ROUTE-NAME=ROUVM2,PROC-NAME=LBSVM2,PATH=*NODE(-
/ NODE-NAME=HNC#NODE,LINE-NAME=HNCLINE1,L3-PROTOCOL=*IP(-
/ IP-ADDR=172.25.226.240)),ATTR=*PAR(ROUTE-SEQUENCE-NUM=1)

/MODIFY-LINE LINE-NAME=HNCLINE1,-
/ AUTO-ROUTE-SWITCHING=*ON,ROUTE-RESWITCHING=*ON
/MODIFY-LINE LINE-NAME=HNCLINE2,-
/ AUTO-ROUTE-SWITCHING=*ON,ROUTE-RESWITCHING=*ON

/BCACT NODE=HNC#NODE,ACT=ONLY
/BCACT PROCESSOR=LBSVM2,ACT=ALL
...
```

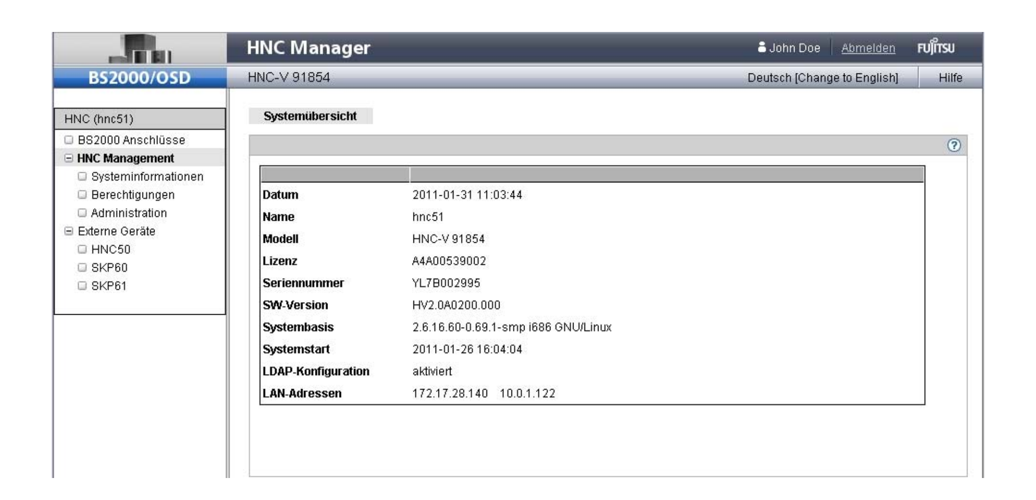
5 HNC verwalten

Alle Funktionen, mit denen Sie den HNC verwalten, sind im HNC-Manager in der Primärnavigation unter *HNC Management* zusammengefasst.

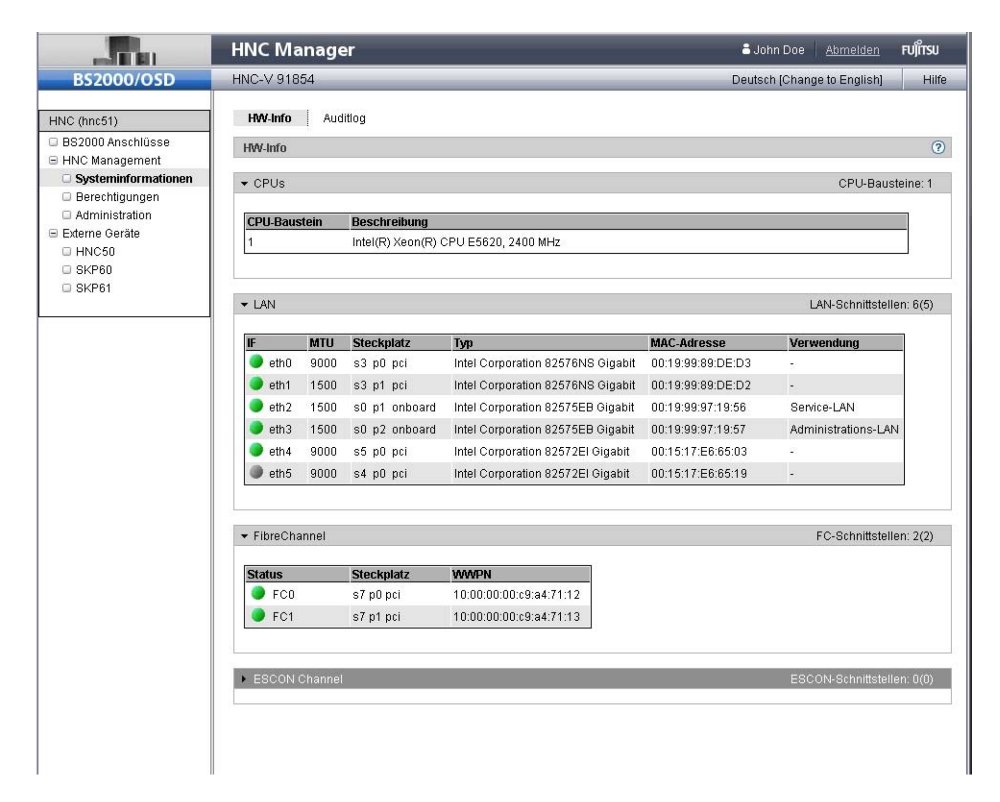
5.1 Informationen über den HNC einholen

Unter *HNC Management>Systeminformationen* zeigt der HNC-Manager den aktuellen HW- und SW-Stand an.

- Die Registerkarte *Übersicht* zeigt die derzeit installierten SW-Stände.



- Die Registerkarte *HW-Info* zeigt Informationen zur aktuellen Hardware.



Der Arbeitsbereich zeigt vier Gruppen, die Sie durch einen Klick in die Überschriftenzeile einzeln auf- (und wieder zu-) klappen können. Im Beispiel sind die Informationen zu den LAN-Anschlüssen ausgeklappt. Erläuterungen zu den Informationen finden Sie in der Online-Hilfe.

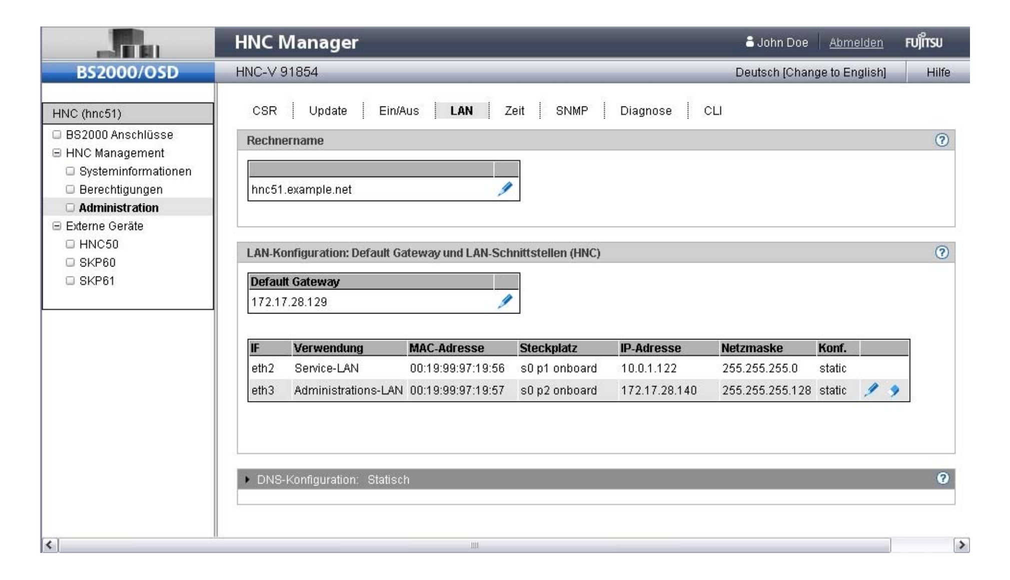
5.2 HNC konfigurieren

Für die Konfiguration des HNC in Ihr Netzt bietet der HNC-Manager folgende Funktionen:

- „Rechnernamen, Default-Gateway, LAN-Schnittstellen und DNS-Konfiguration verwalten“ auf Seite 41
- „Systemzeit konfigurieren“ auf Seite 42
- „SNMP konfigurieren“ auf Seite 43
- „Links auf externe Geräte verwalten“ auf Seite 45

5.2.1 Rechnernamen, Default-Gateway, LAN-Schnittstellen und DNS-Konfiguration verwalten

Die Registerkarte *LAN* unter *HNC Management>Administration* zeigt die aktuelle LAN-Konfiguration des HNC.



Der Arbeitsbereich gliedert sich in folgende Gruppen:

- Rechnername
- LAN-Konfiguration: Default-Gateway und LAN-Schnittstellen
- DNS-Konfiguration

Jede Gruppe zeigt die aktuell konfigurierten Werte an und enthält Aktionen zum Ändern (und teilweise auch zum Löschen) von Konfigurationsdaten. Weitere Informationen finden Sie in der Online-Hilfe.

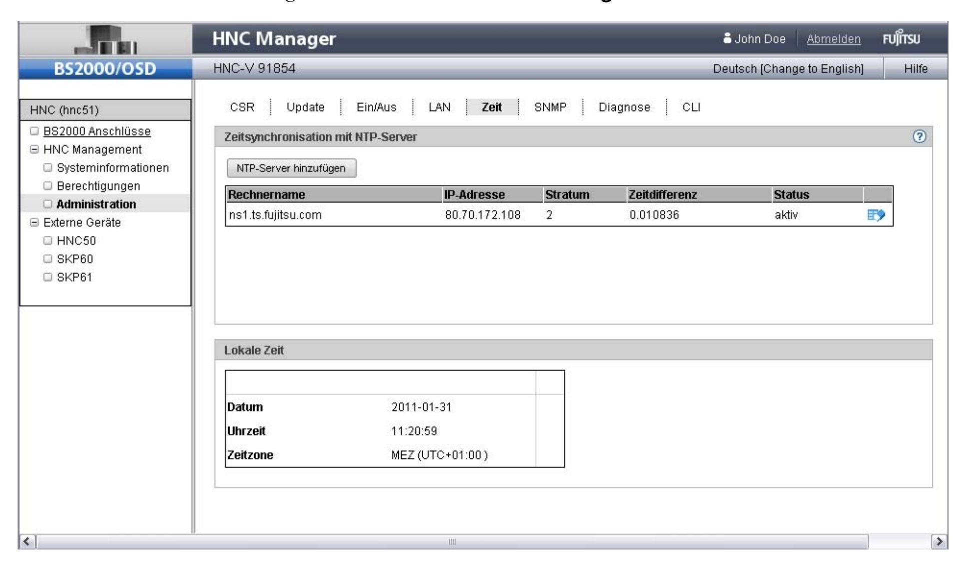


Wenn Sie ein Objekt konfiguriert haben – z.B. die IP-Adresse für das Administrations-LAN – kann die Verbindung zum HNC-Manager abbrechen. Eine neue Verbindung muss anschließend explizit aufgebaut werden. Schließen Sie den Dialog, der in diesem Fall nach Durchführung der Aktion vom System keine Antwort erhält.

5.2.2 Systemzeit konfigurieren

Der HNC hat ein eigenes Zeitmanagement mit einer lokal eingestellten Zeit. Wenn an einem System Zeitabweichungen auftreten, können Sie die lokale Zeit manuell korrigieren. Für eine bessere Zeitgenauigkeit können Sie auch den automatischen Zeitabgleich über NTP (Network Time Protocol) mit einem anderen Server, der z.B. eine funkuhr-genaue Zeit liefert, konfigurieren.

► Wählen Sie *HNC Management > Administration,* Registerkarte *Zeit*.



Im Arbeitsbereich wird unter *Zeitsynchronisation mit NTP-Servern* eine Tabelle der NTP-Server ausgegeben, die für die automatische Zeitsynchronisation definiert wurden. Für den NTP-Server, von dem die Zeit tatsächlich bezogen wird, wird der Zustand aktiv angezeigt. Unter *Lokale Zeit* wird die aktuelle lokale Zeit mit Datum, Uhrzeit und Zeitzone angezeigt.

i

Wenn die Zeit nicht von einem NTP-Server bezogen wird, können Sie die lokale Zeit ändern.

5.2.3 SNMP konfigurieren

SNMP (Simple Network Management Protocol) ist ein Kommunikationsprotokoll für das Netz-, System- und Anwendungsmanagement und ermöglicht die Überwachung des HNC über LAN. Die Überwachung erfolgt durch Management-Stationen, die über das SNMP-Protokoll mit dem im HNC installierten SNMP-Agenten kommunizieren.

Der SNMP-Agent unterstützt folgende MIBs:

- RFC 1213 (MIB-II)
- MIBs mit privaten Traps

Private Traps werden z.B. in folgenden Fällen verschickt:

- beim Neustart des HNC
- beim Umschalten in den Wartungsmodus
- beim Zurückschalten in den aktiven Modus
- beim Senden eines Test-Traps

Um die Traps interpretieren zu können, müssen folgende MIBs an der Management-Station importiert werden:

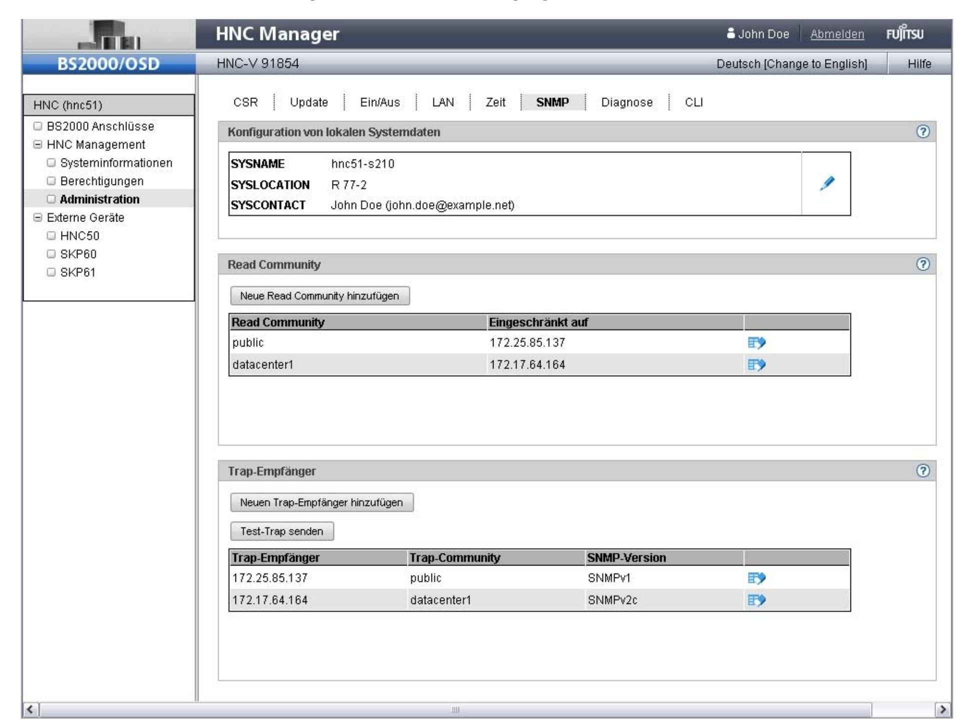
- `/usr/share/snmp/mibs/FTS-HNCSERVER-MIB.txt`
- `/usr/share/snmp/mibs/SNI-MIB.txt`

Der Zugriff ist z.B. mit scp (secure copy) möglich.

SNMP-Konfiguration anzeigen

▸ Wählen Sie *HNC Management* > *Administration,* Registerkarte *SNMP.*

Die aktuelle SNMP-Konfiguration wird ausgegeben.



Aktionen für die SNMP-Konfiguration

- Ändern von *SYSNAME*, *SYSLOCATION* und *SYSCONTACT*
- *Read Community* hinzufügen
- *Read Community* entfernen
- *Trap-Empfänger* hinzufügen
- *Trap-Empfänger* entfernen
- *Test-Trap* senden (sofern ein Trap-Empfänger eingetragen ist)

i Die Werte für *Read Community* und *Trap-Empfänger* können nicht geändert werden. Entfernen Sie den zu ändernden Wert zunächst und fügen ihn dann mit dem neuen Wert hinzu.

5.2.4 Links auf externe Geräte verwalten

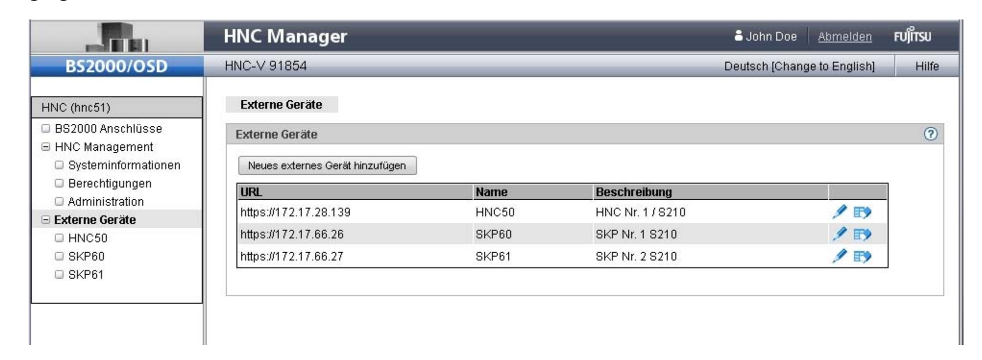
Am HNC lassen sich Links auf die Web-Oberflächen von externen Geräten verwalten. Für jeden Eintrag wird in der Primärnavigation ein Link angezeigt. So können Sie beispielsweise Links zu den anderen HNCs oder SKPs Ihres Rechenzentrums in den HNC-Manager integrieren.

Beim Klick auf einen Link öffnet sich die entsprechende Web-Oberfläche in einem neuen Browser-Fenster, wenn sie für den aufrufenden Administrations-PC erreichbar ist.

Vorhandene externe Geräte ausgeben

► Wählen Sie *Externe Geräte*.

Die Liste der vorhandenen externen Geräte wird im unteren Teil des Arbeitsbereichs ausgegeben.



Aktionen für externe Geräte

- Neues externes Gerät hinzufügen
- Attribute eines externen Gerätes ändern
- Vorhandenes externes Gerät entfernen

5.3 Kennungen verwalten

Ein Administrator verwaltet alle Kennungen am HNC. Er legt neue lokale Kennungen an und ändert oder löscht bestehende Kennungen. Bei Einsatz von zentral verwalteten Kennungen an einem LDAP-Server konfiguriert der Administrator den Zugang zu einer Kennungsdatenbank und gibt zentrale Kennungen am HNC frei.

Die Kennung *sysadm* für den Administrator ist vordefiniert. Sie können weitere Kennungen einrichten oder zulassen.

Alle Kennungen sind gleichberechtigte Administratorkennungen.

„Lokale Kennungen verwalten“ auf Seite 46 beschreibt, wie Sie lokale Kennungen einrichten, ändern und löschen.

Andere Kennungen sind zwar lokal freigegeben, werden aber zentral auf einem LDAP-Server verwaltet (LDAP=Lightweight Directory Access Protocol). Zur Administration dieser Kennungen siehe „LDAP-Kennungen verwalten“ auf Seite 49.

Für lokale Kennungen können Sie Passwörter und Passwortattribute (z.B. zur Gültigkeitsdauer) verwalten. Die Online-Hilfe beschreibt diese Funktionen zur Passwortverwaltung.

5.3.1 Lokale Kennungen verwalten

Alle am HNC lokal eingerichteten Kennungen sind mit dem Lokal-Symbol versehen.

Lokale Kennungen anzeigen

► Wählen Sie *HNC Management* > *Berechtigungen,* Registerkarte *Kennungen*.

Im Arbeitsbereich wird eine Liste der vorhandenen Kennungen ausgegeben.



► Um ausschließlich die lokalen Kennungen anzuzeigen, filtern Sie in der Spalte *Typ* durch Auswahl von *Lokale*.

Die lokalen Kennungen werden angezeigt.

Aktionen für lokale Kennungen

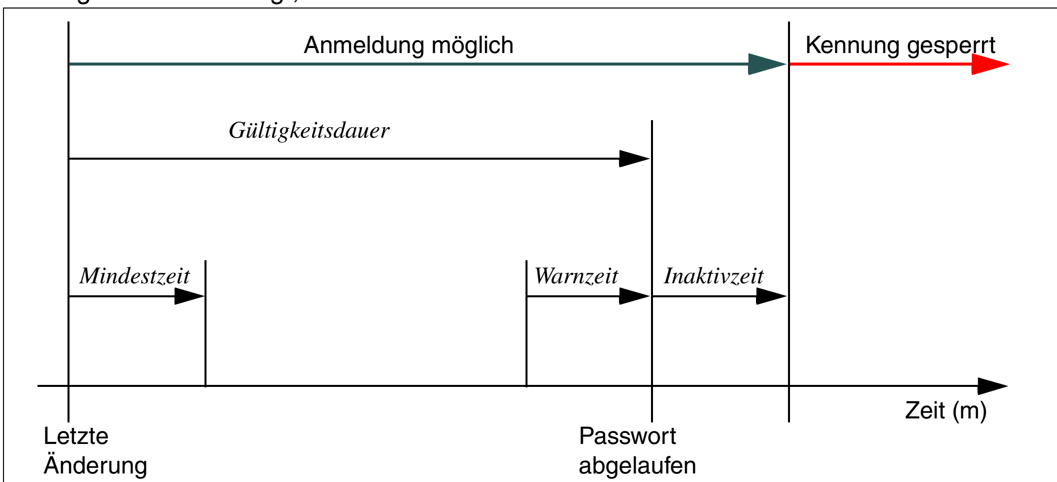
- Lokale Kennung neu einrichten
- Attribute einer lokalen Kennung ändern
- Lokale Kennung löschen
- Passwort verwalten
- Lokale Kennung aktivieren bzw. deaktivieren

5.3.2 Passwörter

Die Passwörter der lokalen Kennungen haben folgende Attribute:
Gültigkeitsdauer, *Warnzeit, Inaktivzeit*:

– Während der Gültigkeitsdauer, die ab dem letzten Setzen des Passworts gilt, ist die Anmeldung unbeschränkt möglich.
– Während der Warnzeit wird eine Warnung ausgegeben, dass das Passwort bald ausläuft. Die Anmeldung ist aber ohne Einschränkungen möglich.
– Während der Inaktivzeit ist das Passwort zwar abgelaufen, eine Anmeldung ist aber trotzdem möglich. Direkt bei der Anmeldung wird eine Passwortänderungen verlangt.
– Nach Ablauf der Inaktivzeit ist die Kennung gesperrt. Sie kann von einer (anderen) Administratorkennung aus oder notfalls durch den Service wieder geöffnet werden.
– Der Wert -1 bei der *Inaktivzeit* führt dazu, dass die Inaktivzeit nicht abläuft.
– Der Wert *99999* für die *Gültigkeitsdauer* bedeutet in der Praxis, dass Sie das Passwort nicht ändern müssen.

Die folgende Grafik zeigt, wie sich diese Zeiten zueinander verhalten.



Wenn Sie neue lokale Kennungen über den HNC-Manager einrichten, so erhalten die von Ihnen vergebenen Passwörter zunächst folgende Attribute:

Kennung	Gültigkeit	Warnzeit	Inaktivzeit	Bemerkung
<name>	60	5	7	

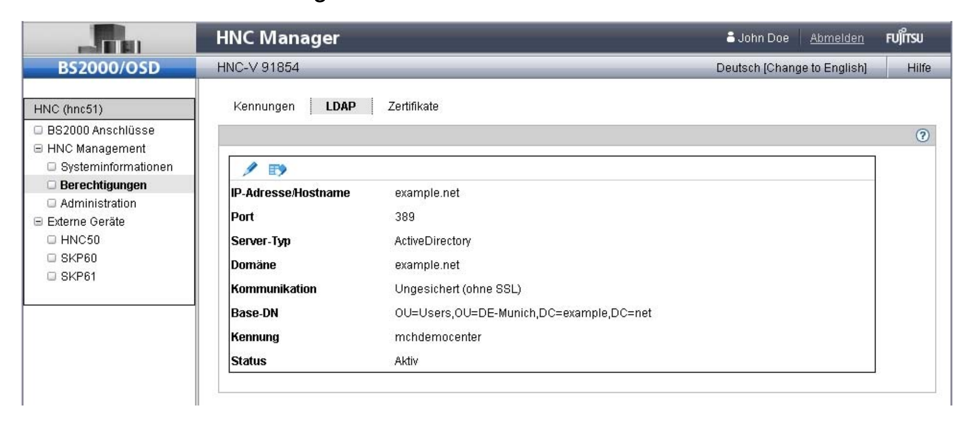
Sie können jederzeit die Attribute (personenbezogener Name und Bemerkung) Ihrer eigenen lokalen Kennung ändern.

5.3.3 Zugang zu einem LDAP-Server einrichten

Sie können den Zugang zum HNC auch über zentral verwaltete Kennungen zulassen (siehe „LDAP-Kennungen verwalten“ auf Seite 49). Diese Kennungen sind zentral auf einem LDAP-Server (Lightweight Directory Access Protocol) eingerichtet und werden ausschließlich dort verwaltet. Die Authentifizierung für eine solche Kennung findet auf dem LDAP-Server statt. Der Einsatz von LDAP-Kennungen am HNC erfordert einen Zugang des HNC zum LDAP-Server. Die nötigen Daten erfahren Sie vom Administrator des LDAP-Servers.

► Wählen Sie *HNC Management* > *Berechtigungen, Registerkarte LDAP.*

Im Arbeitsbereich werden die Zugangsparameter für den konfigurierten LDAP-Server ausgegeben. Falls kein Zugang konfiguriert ist, sind die Parameter leer und nur *Kennung* ist mit `ANONYMOUS` vorbelegt..



Aktionen für den Zugang zu einem LDAP-Server

- Zugang zum LDAP-Server einrichten (diese Aktion wird nur angeboten, wenn noch kein Zugang konfiguriert ist)
- Zugang zum LDAP-Server ändern
- Zugang zum LDAP-Server löschen

5.3.4 LDAP-Kennungen verwalten

LDAP-Kennungen sind in einer Datenbank am LDAP-Server angelegt und werden dort zentral vom Administrator des LDAP-Servers verwaltet. Die Verwaltung an Ihrem HNC beschränkt sich darauf, dass Sie eine bereits existierende LDAP-Kennung am HNC zur Nutzung freigeben oder blockieren. Im HNC werden nur einige Daten für die Kennung angelegt (wie Login-Verzeichnis, die Attribute Name und Bemerkung der Kennung).

LDAP-Kennungen, die denselben Namen haben wie eine lokal eingerichtete Kennung, können Sie am HNC nicht freigeben. Um LDAP-Kennungen zu nutzen, benötigen Sie einen konfigurierten und aktivierten Zugang zum LDAP-Server. (siehe „Zugang zu einem LDAP-Server einrichten“ auf Seite 48). Die notwendigen Daten erfahren Sie vom Administrator des LDAP-Servers.

► Wählen Sie *HNC Management* > *Berechtigungen,* Registerkarte *Kennungen.*

Die Tabelle im Arbeitsbereich zeigt alle Kennungen an, die Zugriff zum HNC besitzen. Die am HNC freigegebenen LDAP-Kennungen sind mit dem LDAP-Symbol versehen.

► Um ausschließlich LDAP-Kennungen anzuzeigen, filtern Sie in der Spalte *Typ* durch Auswahl von *LDAP*.

Aktionen für LDAP-Kennungen

- LDAP-Kennung freigeben
- Attribute einer LDAP-Kennung ändern
- LDAP-Kennung sperren

5.4 CSR-Sicherungen verwalten

Mit einer CSR-Sicherung (CSR = Configuration Save and Restore) sichern Sie Konfigurationsdaten des HNC in einem Archiv. Das Sicherungsarchiv enthält die vollständige Konfiguration des Systems, z.B. die Geräte, die Kennungen und die NTP-Konfiguration. Jedes Sicherungsarchiv hat ein Erstelldatum und einen Archivnamen. Daneben gibt es auch Sicherungen, die vom System angelegt werden, z.B. bei Installation eines Updates. Diese Sicherungen haben selbsterklärende Namen wie `before_online_update`.

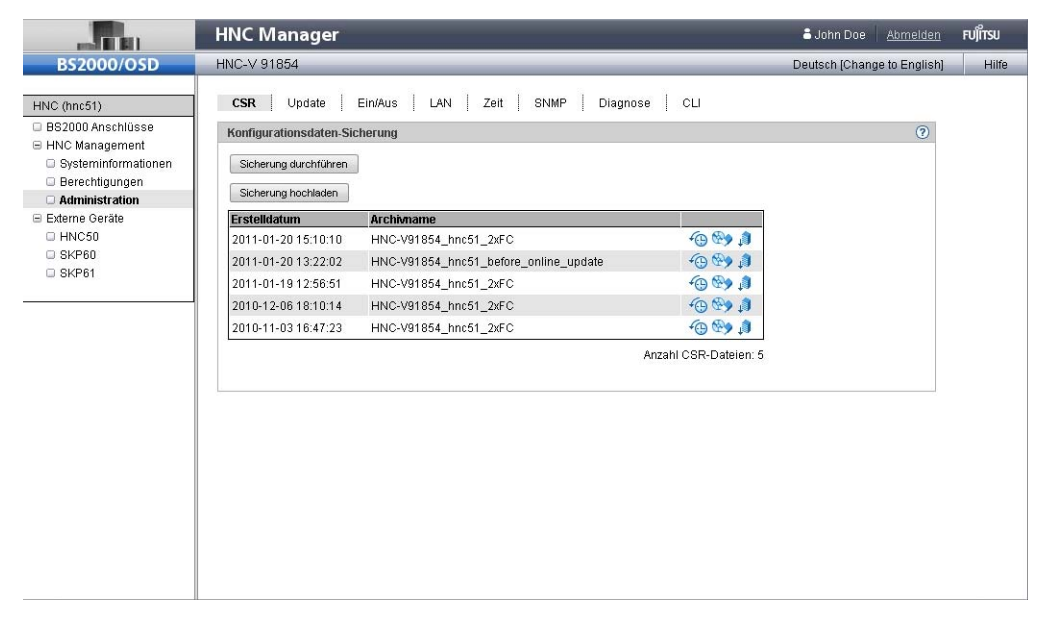
Tipp: Führen Sie nach jeder Konfigurationsänderung eine CSR-Sicherung durch.

Mit einer CSR-Sicherung lässt sich die Konfiguration des HNC zum Zeitpunkt der Sicherung wiederherstellen.

CSR-Sicherungen anzeigen

► Wählen Sie *HNC Management* > *Administration,* Registerkarte *CSR*.

Im Arbeitsbereich wird unter *Konfigurationsdaten-Sicherung* eine Liste der vorhandenen Sicherungsarchive ausgegeben.



Aktionen für CSR-Sicherungen

- CSR-Sicherung durchführen
- Sicherung wiederherstellen

  i Die Wiederherstellung verursacht einen Neustart (Reboot) des HNC.

- Sicherung herunterladen
- Sicherung hochladen
- Sicherungsarchiv löschen

5.5 HNC ein- und ausschalten

Sie können den HNC über den HNC-Manager remote direkt oder zeitgesteuert ein- oder ausschalten. Die Funktion dazu finden in der Registerkarte *Ein/Aus* unter *HNC Management>Administration*.

Sie können den HNC auch kontrolliert herunterfahren, indem Sie den Ein-/Ausschaltknopf am Gerät einmal kurz drücken. Wenn Sie den Ein-/Ausschaltknopf lange drücken, schaltet sich der HNC sofort aus. In diesem Fall kann es zu einem Datenverlust am HNC kommen. Deshalb sollte dies nur in Notfällen geschehen.



Beim Herunterfahren ohne Neustart können Sie den HNC **nicht** aus der Ferne wieder hochfahren. Zum Einschalten des HNC müssen Sie den Einschaltknopf des HNC drücken.

6 Diagnose und Wartung

Für die Wartung des HNC bietet der HNC-Manager unter *HNC Management>Administration* folgende Funktionen:

- Wartungskonzept
- Updates
- Diagnose
- Systemprotokoll

6.1 Wartungskonzept

Der Service führt die vertraglich vereinbarten Service-Tätigkeiten in der Regel aus der Ferne als Remote-Service durch. Alternativ kann er Service-Tätigkeiten auch vor Ort beim Kunden durchführen. Die Wartung der Hardware oder die Behebung von Hardware-Problemen ist nur vor Ort möglich.

Der HNC besitzt keine eigene Anbindung an den Remote Service. Er kann aber mittelbar über den SKP angeschlossen werden, der eine Anbindung an den Remote Service besitzt.

Der Anschluss des HNC an einen SKP wird in der Regel über eine LAN-Verbindung (Service-LAN) realisiert. HNCs vom Typ HNC-IV können auch über die V24-Schnittstelle angeschlossen werden. Der Anschluss des HNC an einen SKP erfordert Konfigurationsmaßnahmen und wird durch den Service realisiert.

6.1.1 Remote-Service

Bereits bei der Systeminstallation oder bei Inbetriebnahme der HNCs und SKPs im Kundenrechenzentrum konfiguriert der Service den Remote-Service unter Berücksichtigung der Kundenwünsche. Die Konfiguration kann beispielsweise so vorgenommen werden, dass Sie als Administrator sämtliche Service-Aktivitäten beobachten (zwingender Einsatz eines sogenannten Schattenterminals), siehe hierzu auch das SKP Handbuch [7].

Der Remote-Service stellt sicher, dass bei Auftreten einer Störung ein Service-Call an die Service-Zentrale gesendet wird (ausgehende Verbindung).
Der Service kann die Verbindung zum HNC auch von sich aus aufnehmen (eingehende Verbindung), wenn er eine Störung beheben oder präventive Maßnahmen durchführen will (Änderungen, Updates, Diagnose, etc.).

Wenn es unbedingt erforderlich ist, können Sie als Administrator die Remote-Service-Konfiguration des SKP ändern oder in einen gerade laufenden Service-Vorgang eingreifen. Die Änderungen der Remote-Service-Konfiguration am SKP haben Auswirkungen auf die Service-Fähigkeit Ihres HNC.



Wichtig!
Die Änderung der Remote-Service-Konfiguration ist zwischen den Administratoren des SKP und des HNC sowie der Service-Zentrale unbedingt abzustimmen, da ansonsten die Service-Fähigkeit der von Ihnen betreuten Systeme (HNC, SKP und S-Server) gefährdet ist.
Sicherheitsrelevante Aspekte des Remote-Service sind im Sicherheitshandbuch [6] beschrieben.

Service-Kennungen

Um seine Arbeit durchführen zu können, meldet sich der Service (remote oder lokal) unter der dafür vorgesehenen Service-Kennung an. Dem Service steht die geschützte Kennung *service* im Basisbetriebssystem zur Verfügung.

6.1.2 Aufgaben des Service

Der Service hat folgende Aufgaben:

- Diagnose und Entstörungen
- Wartungsarbeiten Software (Update)
  - Bereitstellung und Installation Service Pack
  - Bereitstellung und Installation Hot Fix
  - Bereitstellung Security Fix
- Wartungsarbeiten Hardware
  - Hochrüstungen Software/Firmware
  - Modell-Upgrade
- Erhöhung der Anzahl der Lizenzen/MAC-Adressen für ZASLAN-Anschlüsse (für die Erhöhung der Konnektivität von BS2000-Systemen)
- Hochrüstungen Hardware

6.1.3 Aufgaben des Kunden

Zur Wahrnehmung der Service-Tätigkeiten benötigt der Service in einigen Fällen Ihre Unterstützung vor Ort. Als Kunde haben Sie innerhalb des Wartungskonzepts folgende Aufgaben:

- Zugang zum HNC ermöglichen
  - Remote-Service-Zugang ggf. vom Administrator des SKP öffnen lassen (wird für Service- und Wartungskonzept vorausgesetzt)
  - Zugang zum Rack ermöglichen (z.B. zur lokalen Konsole)
- Unterstützung des Service bei Software/Firmware-Updates des HNC; jeweils nach Absprache mit dem Service fallen gegebenenfalls folgende Aufgaben an:
  - Übertragen der Updates von CD/DVD auf Platte
  - Hochladen Service Pack
  - Hochladen Hot Fix
  - Hochladen und Installation Security Fix
- Erzeugung und Lieferung von Diagnose-Unterlagen

Geben Sie bei der Kommunikation mit dem Service Ihren HNC eindeutig über die Seriennummern an. Die Seriennummern finden Sie im HNC-Manager unter *HNC Management*, Registerkarte *Systemübersicht*.

Die Seriennummer lautet YLEC<xxxxxx> (für freistehende Systeme) bzw. YLED<xxxxxx> (für Rack-Einschübe).

Hinweis: Bei älterer Hardware (HNC-IV) steht die anzugebende Seriennummer auf dem Typ-/Leistungsschild und beginnt mit FT gefolgt von einer laufenden Nummer.

6.2 Updates

Der Software-Stand enthält neben der Systemversion auch die Updates, die am HNC installiert sind. Dabei werden folgende Update-Arten unterschieden:

- Service Pack
- Security Fix
- Hot Fix

Im Feld *SW-Version* der Systemübersicht wird die Version der HNC-Software einschließlich des Update-Standes angezeigt.

Der Software-Stand hat also folgende Bestandteile:

Bestandteil	**Beispiel**	**Beschreibung**
Version	2.0A	
Revision	REV=003	Update-Stand
Service Pack	SP=01	– Ein Service Pack hat eine laufende Nummer (01 im Beispiel) – Service Packs erhöhen den Update-Stand
Security Fix	SF=01	– Security Fixes sind einem Versions- und Update-Stand zugeordnet – Security Fixes haben pro Versions- und Update-Stand eine laufende Nummer (01 im Beispiel)
Hot Fix	A0562581-H01	– Hot Fixes sind einem Versions- und Update-Stand zugeordnet – Hot Fixes beinhalten im Namen die Nummer einer so genannten Problemmeldung (A0562581 im Beispiel) sowie eine laufende Nummer (H01 im Beispiel)

Updates werden als Dateien folgenden Typs geliefert:

- `iso.gz` für Dateien, die vom Download-Server heruntergeladen werden können
- `iso` für Dateien, die auf CD/DVD geliefert werden

Die Dateien mit den Updates haben folgende Namenskonventionen:

Security Fix	z.B. `HV2.0A01.01.iso[.gz]` Der Security Fix mit der Nummer `01` ist dem Versions- und Update-Stand `2.0A REV=01` zugeordnet.
Hot Fix	z.B. `HV2.0A01.A0562581-H01.iso[.gz]` Der Hot Fix mit dem Namen `A0562581-H01` ist dem Versions- und Update-Stand `2.0A REV=01` zugeordnet.
Service Pack	z.B. `HV2.0A0101.iso[.gz]` Das Service Pack setzt den Versions- und Update-Stand auf `2.0A REV=0101`. Die Zählung der Security Fixes wird neu initialisiert (auf `000` gesetzt).

Der Buchstabe `H` im Dateinamen weist auf die Zugehörigkeit zum HNC hin.

6.2.1 Aufgaben und Zuständigkeiten

Die folgende Tabelle zeigt die Aufgaben des Administrators und des Service sowie den zeitlichen Ablauf bei der Installation und Verwaltung von Updates.

Update-Art	**Administrator**	**Service**
Security Fix	alle Aufgaben werden vom Administrator ausgeführt: – Bedarf klären – Wartungsfenster bereitstellen (falls nötig) – Security Fix beschaffen – Security Fix in das System übertragen – Security Fix installieren und gegebenenfalls explizit durch Neustart aktivieren	keine Aufgabe
Service Pack	– Bedarf klären – Wartungsfenster bereitstellen – Service Pack beschaffen – Service Pack in das System übertragen	– Bedarf klären – Service Pack installieren (via Teleservice oder vor Ort)
Hot Fix	– Bedarf klären – Wartungsfenster bereitstellen (falls nötig) – Hot Fix beschaffen (oder der Service) – Hot Fix in das System übertragen (oder der Service)	– Bedarf klären – Hot Fix beschaffen – Hot Fix in das System übertragen (via Teleservice oder vor Ort) – Hot Fix installieren (via Teleservice oder vor Ort)

6.2.2 Updates beschaffen

Security Fixes stellt Fujitsu in der Regel im Internet auf seinem Download-Server bereit. Die erforderlichen Updates laden Sie auf Ihren PC herunter.
Alternativ erhalten Sie Updates wie Service Packs oder Hot Fixes z.B. auch per E-Mail oder auf CD/DVD.

6.2.3 Updates verwalten

Um Software-Updates zu installieren, müssen sie am HNC verfügbar sein. Die folgende Arten von Updates können Sie auf den HNC transferieren und dort verwalten:

- Security Fix

  Ein Security Fix enthält alle sicherheitsrelevanten Updates für das Linux-basierte Betriebssystem, die seit dem letzten Service Pack erschienen sind. Security Fixes schützen das jeweilige System z.B. gegen unbefugtes Eindringen oder gegen Angriffe von Außen. Ob Sie aktuelle Security Fixes installieren, ist abhängig von Ihren Sicherheitsanforderungen und davon, ob Zugriffe auf den HNC nur über das abgeschottete Administrations-LAN oder auch von Außen möglich sind. Die funktionelle Nutzung des HNC ist auch ohne aktuelle Security Fixes gewährleistet.

- Service Pack

  Ein Service Pack enthält eine Sammlung von Korrekturen für das Linux-basierte Betriebssystem. Enthalten sind alle vorangegangenen Service Packs und Security Fixes, sowie ausgewählte Hot Fixes. Die Installation erfolgt durch den Service.

- Hot Fix

  Ein Hot Fix enthält eine Korrektur, mit der ein dringendes Problem in Ihrem System möglichst rasch behoben werden kann. Die Installation erfolgt durch den Service.

6.2.4 Aktionen für Updates

Für die verschiedenen Update-Arten können Sie folgende Aktionen ausführen:

Update-Art	Update von CD/DVD übertragen	Update anzeigen	Freigabe-mitteilung anzeigen	Update hochladen	Update installieren
Security Fix	X	X	X	X	X
Hot Fix	X	X	X	X	
Service Pack	X	X	X	X	

Wählen Sie *HNC Management > Administration*, Registerkarte *Update*.

Die Aktionen laufen für alle Update-Arten ähnlich ab. Bei der Installation eines Update wird implizit eine Konfigurationsdaten-Sicherung (CSR-Sicherung) in die tar-Datei `before_online_update` (mit Zeitstempel) durchgeführt. Somit bleibt nur die letzte Konfigurationsdaten-Sicherung erhalten. Nähere Informationen finden Sie in der Online-Hilfe.

6.3 Den Service unterstützen

Der HNC besitzt keine eigene Remote-Service-Anbindung, sondern diese wird durch die korrekte Anbindung an einen SKP realisiert, der eine eigene Remote-Service-Anbindung besitzt. Somit hängt die momentane Service-Fähigkeit des HNC von der des SKP ab.

In einigen Fällen kann es erforderlich sein, dass zur Unterstützung des Service die Konfiguration des Zugangs am SKP zu ändern ist (z.B. Öffnen des Zugangs), oder dass in einen gerade laufenden Service-Vorgang eingegriffen werden muss.

Die entsprechenden Funktionen stehen auf dem SKP dem Administrator (und in geringerem Umfang dem Operator) zur Verfügung. Details finden Sie im SKP-Handbuch [7] im Abschnitt "Den Service unterstützen".



Die Änderung der Remote-Service-Konfiguration ist zwischen den Administratoren des SKP und des HNC sowie der Service-Zentrale unbedingt abzustimmen, da ansonsten die Service-Fähigkeit der von Ihnen betreuten Systeme (HNC, SKP und S-Server) gefährdet ist.

Sicherheitsrelevante Aspekte des Remote Service sind im Sicherheitshandbuch [6] beschrieben.

6.4 Diagnosedaten

In einer Fehlersituation ist es sinnvoll Diagnosedaten zu erzeugen und sie zur Auswertung an die Service-Zentrale zu senden.
Die Diagnosedatei ist ein komprimiertes tar-Archiv und enthält wichtige Logging-, Trace- und Konfigurationsdateien.

► Wählen Sie *HNC Management* > *Administration,* Registerkarte *Diagnose.*



Im Arbeitsbereich wird unter *Dateiname* der Name einer bereits vorhandenen Diagnosedatei ausgegeben: DIAGtar.<date>.<time>.gz.

Ein „-“ statt eines Dateinamens zeigt an, dass noch keine Diagnosedaten erstellt wurden.

Aktionen für Diagnoseunterlagen

- Neue Diagnosedaten erzeugen



Achtung:
Eine bereits vorhandene Diagnosedatei wird dabei überschrieben. Laden Sie gegebenenfalls vorher die bereits vorhandene Datei auf Ihr lokales System herunter.

- Diagnosedaten auf den PC herunterladen

6.5 Systemprotokoll (Auditlog)

Die Funktion Auditlog protokolliert am HNC alle Aktionen, die über den HNC-Manager oder das CLI ausgeführt werden und eine Konfigurations- oder Zustandsänderung bewirken. Lediglich reine Ausgaben werden nicht protokolliert.

Die Protokollierung erfolgt automatisch. Einträge werden in eine Datei mit Namen *auditlog* geschrieben. Der Inhalt der Protokolldatei wird monatlich oder bei Überschreitung der maximalen Größe von 10 MB gesichert und komprimiert. Die gesicherten Dateien haben den Namen *auditlog.<yyyymmdd>.bz2* (*yyyymmdd*: Zeitstempel in der Form Jahr-Monat-Tag). Maximal 36 Protokolldateien werden archiviert, so dass in der Regel ein Zeitraum von 3 Jahren überblickt werden kann.

Sie können die Protokolldateien von Auditlog ansehen und auf Ihren PC herunterladen:

► Wählen Sie *HNC Management* > *Systeminformationen,* Registerkarte *Auditlog.*



Aufbau Auditlog

Jeder interne CLI-Aufruf, der für eine Aktion ausgeführt wird, erzeugt eigene Protokolleinträge (der Start und das Ergebnis). Deshalb stehen für eine Aktion oft mehrere Einträge im Protokoll.

Eine Zeile im Auditlog ist folgendermaßen aufgebaut:

```
<Zeitstempel> <Systemname> <Kennung>_[Web-Identifikation] <Eintragstyp>
<Kommandotext>
```

`Zeitstempel` Zeitpunkt des Eintrags im Format <yyyymmdd.hhmmss>

`Systemname` Name des Rechners, auf dem die Aktion ausgeführt wurde.

`Kennung` Kennung, unter der die Aktion ausgeführt wurde. Der HNC-Manager (GUI) läuft unter der Kennung wwwrun. Deshalb wird in diesem Fall die Web-Identifikation (GUI-Kennung + IP-Adresse) angehängt.

`Eintragstyp` Beschreibt die Aktion und kann folgende Werte annehmen:

`start`	Start einer Aktion auf CLI-Ebene
`sqmstart`	Start einer Aktion auf GUI-Ebene
`rc=RC`	Ergebnis einer Aktion auf CLI-Ebene
`sqmrc=RC`	Ergebnis einer Aktion auf GUI-Ebene
`access`	Anmeldung auf CLI-Ebene
`sqmaccess`	Anmeldung auf GUI-Ebene
status	Statusmeldung einer Komponente
`entry`	Interner Aufruf

`Kommandotext` Informationen zur Aktion

CLI: Das Kommando wird mit allen Parametern protokolliert.

GUI: Die Aktion wird wie im GUI und auch in der eingestellten Sprache protokolliert.

Ausnahmen: Sicherheitsrelevante Daten wie Passwörter werden nicht protokolliert.

Eine einfache Aktion besteht aus 2 Zeilen, aus dem Start der Aktion (start) und aus dem Ergebnis (rc=). Eine komplexe Aktion schachtelt einfache Einträge gemäß den internen Aufrufen.

Beispiel

Der Benutzer sysadm ändert sein Passwort:

```
20101115.141626 abgsouth wwwrun_sysadm_217.9.101.18 sqmstart
Aktion=Passwortverwaltung; Kennung=sysadm; Passwort=******;
20101115.141626 abgsouth wwwrun start passwd -S sysadm
20101115.141626 abgsouth wwwrun rc=0 passwd -S sysadm
20101115.141626 abgsouth wwwrun start passwd --stdin sysadm
20101115.141626 abgsouth wwwrun rc=0 passwd --stdin sysadm
20101115.141626 abgsouth wwwrun_sysadm_217.9.101.18 sqmrc=0
Aktion=Passwortverwaltung; Kennung=sysadm; Passwort=******; --> Das Passwort
für die Kennung sysadm wurde erfolgreich geändert.
```

Aktionen für Auditlog

- Ansicht einzelner Auditlog-Dateien, filtern ist möglich
- Auditlog auf den PC herunterladen

Literatur

Die Handbücher sind online unter *http://manuals.ts.fujitsu.com* zu finden oder in gedruckter Form gegen gesondertes Entgelt unter *http://manualshop.ts.fujitsu.com* zu bestellen.

[1] **BS2000/OSD-BC**
Systeminstallation
Benutzerhandbuch

[2] **BS2000/OSD-BC**
Einführung in die Systembetreuung
Benutzerhandbuch

[3] **VM2000**
Virtuelles Maschinensystem
Benutzerhandbuch

[4] **openNet Server** (BS2000/OSD)
BCAM
Benutzerhandbuch

[5] **BS2000/OSD-BC**
Kommandos
Benutzerhandbuch

[6] **SQ Server/SKP/HNC**
Sicherheitshandbuch

[7] **SKP**
Benutzerhandbuch

Stichwörter

A
abmelden
 CLI 31
 HNC-Manager 21
Administrations-LAN 15
Änderungen 8
Anmeldefenster 20
anmelden
 CLI 31
 HNC-Manager 20
Applets 19
Arbeitsbereich 23
Arbeitsweise des HNC 13
Auditlog 61
 Aktionen 62
 Aufbau 61
auditLog (Kommando) 32

B
BCAM 36
Benutzerkennung siehe Kennung
Benutzerverwaltung 46
BS2000-Anschlüsse 15, 33
BS2000-Gerät (emuliert), Eigenschaften 35
BS2000-MAC-Adresse 35
BS2000-MN, LOCLAN-Gerät 36

C
CLI 19, 31, 32
 Zugang beenden 31
 Zugang öffnen 31
cli_info (Kommando) 32
Command Line Interface 19, 31, 32
Configuration Save and Restore 50
Cookies 19
CSR-Sicherung
 anzeigen 50
 Archiv löschen 51
 durchführen 51
 herunterladen 51
 hochladen 51
 verwalten 50
 wiederherstellen 51

D
Darstellungsmittel 9
Datenbank
 für Kennungen 46, 49
Default Gateway 41
Diagnosedaten erzeugen 60
Dialog 25
Domain Name System 41
Download-Server 56

E
Ein- und ausschalten 52
ESCON-Controller 14, 35
externes Gerät, Link im HNC-Manager 45

F
Fehler
 im HNC-Manager 30
Fenster-Typen 22
Fibre Channel 14, 35
Filter 27

G
Gerät
 extern 45
Graphical User Interfac 19

GUI 19
Gültigkeitsdauer 47

H
Hardware, HNC 16
Hauptfenster 23
HNC
  ein-/ausschalten 52
  Hardware 16
  Konfiguration 41
  Prinzipielle Arbeitsweise 13
  Systemzeit konfigurieren 42
  Wartung 53
HNC-Manager
  abmelden 21
  anmelden 20
  Fehler 30
  Oberfläche 22
  Sprache 20
hochladen
  CSR-Sicherung 51
Hot Fix 56, 58

I
Inaktivzeit 47
init (Kommando) 32
IP-Adresse
  BCAM bekanntgeben 36

J
Java Runtime Environment 19
JavaScript 19

K
Kanal Typ-S siehe ESCON
Kennung 21, 46
  aktivieren 47
  ändern 48
  Attribute ändern 47
  deaktivieren 47
  LDAP-Kennung verwalten 49
  lokal 46
  löschen 47
  neu einrichten 47
  sysadm 46
  verwalten 46
Kennungsverwaltung 46
Kommando
  anzeigen, cli_info 32
  auditLog 32
  cli_info 32
  init 32
Konfiguration, HNC 41
Kopfbereich 23

L
LAN-Schnittstelle (X2000) 41
LDAP-Kennung
  verwalten 49
LDAP-Server 46
  Zugang einrichten 48
Lightweight Directory Access Protocol 46
Linux-Version 17
Lizenzen für Open-Source-Software 2
LOCLAN 14

M
MAC-Adresse 14
MARS
  Open-Source-Lizenzen 2
Mnemonik 15

N
Navigieren 27

O
Online-Hilfe 28
Open-Source-Software
  Lizenzen 2

P
Parameterbereich 25
Passwort 21
  verwalten 47
PC 19
Primärnavigation 23
Primergy-Server 16

R
Read Community 44
Registerkarte 23
    CSR 50
    Kennungen 46
    LDAP 48
    SNMP 43
    Systemzeit 42
Remote Service 17
Revision 56

S
S-Server 9
Security Fix 17, 56, 58
Sekundärnavigation 23
Server
    Download 56
Service
    Aufgaben 54
Service Pack 56, 58
Session 21
Session-ID 21
Simple Network Management Protocol (siehe SNMP) 43
SLAN (shared LAN) 14
SNMP 43
    konfigurieren 43
SOF-Datei 36
Software
    Stand 56
    Update 56
Sortieren, Tabelle 27
Sprachoptionen 23
Standardkennungen, Passwort 21
sysadm (Administrator-Rolle) 46
System
    Protokoll 61
    Version 56
    Zeit 42
Systemzeit siehe Zeitsynchronisation

T
Tabelle
    filtern 27
    sortieren 27
Terminal-Fenster
    öffnen 31
    schließen 31
Titelzeile 23
Trap-Empfänger 44

U
Unit-ID 36
Update 56
    Aufgaben 57
    beschaffen 58
    Zuständigkeiten 57
Update-Stand 56, 57

V
VCA 11, 15
Verbindungstyp
    LOCLAN 14
    ZASLAN 14
Virtual Channel Adapter 11, 15
Virtuelle WWPN 36

W
Warnzeit 47
Wartung, HNC 53
WWPN (World Wide Port Name) 14, 36

X
X2000
    Open-Source-Lizenzen 2

Z
ZASLAN 14
Zeitmanagement 42
Zeitsynchronisation
    anzeigen 42
    Systemzeit konfigurieren 42
    Systemzeit, lokal 42
Zugang
    Remote Service 17